PROPUESTA PLAN DE SEGURIDAD INFORMÁTICA PARA LA SECRETARIA EJECUTIVA DEL CONVENIO ANDRÉS BELLO - SECAB

MARIA ALEJANDRA DEL PILAR SUAREZ ROJAS

UNIVERSIDAD PILOTO DE COLOMBIA
FACULTAD DE INGENIERIA
ESPECIALIZACION EN SEGURIDAD INFORMÁTICA
BOGOTA D.C.
2015

PROPUESTA PLAN DE SEGURIDAD INFORMÁTICA PARA LA SECRETARIA EJECUTIVA DEL CONVENIO ANDRÉS BELLO - SECAB

MARIA ALEJANDRA DEL PILAR SUAREZ ROJAS

Proyecto de Grado para optar por el título de
Especialista en Seguridad Informática

Asesor
Álvaro Escobar
Director Especialización en seguridad Informática

UNIVERSIDAD PILOTO DE COLOMBIA
FACULTAD DE INGENIERIA
ESPECIALIZACION EN SEGURIDAD INFORMÁTICA
BOGOTA D.C.
2015

Nota de Aceptación

_____

_____

Firma del presidente del Jurado

_____

Firma del Jurado

_____

Firma del Jurado

Bogotá 19 de Octubre del 2015

CONTENIDO

pág.

pág.

pág.

pág.

LISTA DE CUADROS

pág.

LISTA DE FIGURAS

pág.

LISTA DE ANEXOS

pág.

GLOSARIO[1]

ACTIVO: Cualquier cosa que tenga valor para la organización.

AMENAZAS. Es todo aquello con lo que se puede atentar contra la seguridad, bien sean acciones o elementos de los cuales se vea comprometida la integridad de los activos; dichas amenazas pueden surgir a partir de vulnerabilidades que suelen ser aprovechadas dentro de la organización, con el fin de obtener algún tipo de beneficio.

ANÁLISIS DE RIESGOS: Uso sistemático de la información para identificar las fuentes y estimar el riesgo

CONTROL: Medios para gestionar el riesgo, incluyendo políticas, procedimientos, directrices, prácticas o estructuras de la organización que pueden ser administrativas, técnicas o de gestión.

EVALUACIÓN DE RIESGOS: Todo proceso de análisis y valoración del riesgo.

POLÍTICA: Toda intención y directriz expresada formalmente por la dirección.

RIESGO: Posibilidad de que se produzca un impacto, sobre un activo de la organización.

VULNERABILIDAD: Debilidad de un activo o grupo de activos que puede ser aprovechada por una o más amenazas.

[1] Norma Técnica Colombiana NTC-ISO/IEC 27002 pág. 1,2 y 3.

INTRODUCCIÓN

La información es considerada como el activo de mayor importancia, sin dejar de lado el medio que le contiene, antiguamente dicha información se constituía en papel por lo cual se implementaba una protección física para asegurar dicho activo, pero hoy en día existen diferentes medios para almacenar información: medios extraíbles, bases de datos, servidores en la nube, entre otros.

En la presente propuesta se realiza el planteamiento de diseño de un Plan de Seguridad Informática para la Secretaria Ejecutiva Del Convenio Andrés Bello, cabe resaltar que la importancia de este órgano del gobierno radica en la información que produce y gestiona, haciéndola un insumo vital que es imprescindible proteger; por tal razón, se requiere garantizar las condiciones para su eficiencia y eficacia, estructurando un modelo de seguridad informática que permita plantear soluciones a diferentes problemáticas que podrían afectar la operación normal de este importante organismo.

No obstante, la SECAB no cuenta con ningún tipo de control, ni documentación para las contingencias a las que se encuentra expuesta por los diferentes riesgos existentes, en este sentido, se busca la aprobación de un Plan de Seguridad Informática dentro de la organización que estructure normativas para minimizar los riesgos en la infraestructura y la información originados por las amenazas constantes; con este plan se pueden disminuir las vulnerabilidades dentro de la organización y construir un escudo protector.

Es preciso mencionar que, adicionalmente se implementará el diseño estructural del Sistema de Gestión de la Seguridad de la información tomando como referente la norma técnica ISO 27000 series. Todo lo anterior sujeto a la aprobación de la Secretaria Ejecutiva y el Ministro presidente.

1. JUSTIFICACIÓN

La SECAB por ser un organismo internacional de integración Educativa, Científica, Tecnológica y Cultural en 12 países, durante su participación en las diferentes instancias, se mantiene en la necesidad de ofrecer disponibilidad, integridad y confidencialidad, garantizando así su óptimo y continuo funcionamiento.

Actualmente la SECAB, no cuenta con planes de recuperación en información eficientes, si bien posee una infraestructura, esta es obsoleta en cuanto a hardware en la mayoría de los equipos en funcionamiento y cuenta con Sistemas de Información sin actualizaciones desde hace más de 3 años, es por ello que es indispensable contar con estrategias, planes de seguridad y medidas que puedan garantizar la funcionalidad de los activos que se encuentran dentro de la organización de manera adecuada, con el fin de que ante un caso eventual se puedan aplicar las acciones y medidas necesarias que mitiguen el impacto de pérdida y operatividad de la SECAB.

En ese sentido, la importancia y pertinencia de la presente investigación, radica en la necesidad que tiene la SECAB de contar con un plan estratégico en cuanto a la seguridad se refiere, para así mantener salvaguardados sus activos de mayor importancia.

2. FORMULACIÓN DEL PROBLEMA

Es evidente en el diario vivir que la evolución tecnológica con el pasar del tiempo se vuelve más extensa y que esta no tarda años, solo bastan algunas horas para darse cuenta que tras esta evolución, los ataques se vuelven más comunes, comprometiendo los activos, la prestación de servicios y todo lo que se involucre dentro de las actividades relacionadas en el convenio.

Es preciso preguntarse, ¿Qué pasaría si los activos no se encuentran con la disponibilidad necesaria? o ¿Si la información no contará con la integridad para los Ministros en las rendiciones de cuentas? o ¿Si la información tildada como confidencial entre Ministerios y SECAB se filtrara a personas o entidades que no estuvieran involucradas con el organismo?

En ese sentido, la evolución cobra una importancia cardinal, pues esta, no solo da alcance para mejorar la parte tecnológica del organismo, sino que también, está a disposición de individuos que pretenden ejercer algún control y seguridad sobre aquellos activos que son de gran importancia, permitiendo así, comprometer la continuidad o en algún caso dado el buen nombre de la organización.

Teniendo en cuenta lo anterior se plantea la siguiente pregunta de investigación:

¿De qué manera se puede contribuir a la mitigación de riesgos y protección de los activos tecnológicos de la SECAB?

3. OBJETIVOS

3.1 OBJETIVO GENERAL

Proponer un plan de Seguridad Informática que permita desarrollar operaciones seguras; así como, el aseguramiento de la integridad física, el control de los sistemas de información, y la protección de activos de la Secretaría Ejecutiva del Convenio Andrés Bello (SECAB).

3.2 OBJETIVOS ESPECÍFICOS

- Elaborar un relevamiento y diagnóstico de la situación actual de la SECAB en relación con el grado de desarrollo de su sistema de gestión de la seguridad de la información (SGSI).

- Diseñar estructuralmente el sistema de gestión de la seguridad de la información tomando como referente la norma técnica ISO 27002, mediante la adaptación de las secciones que aplican de la norma a la naturaleza y misión de la SECAB, a partir del diagnóstico realizado.

- Formular una propuesta base a un plan de seguridad informática que contemple las diferentes acciones por acometer definidas a partir del diagnóstico realizado y del diseño del SGSI de la SECAB.

4. MARCO TEÓRICO

Con el pasar del tiempo la seguridad informática ha tomado una mayor importancia debido a los avances tecnológicos, las posibilidades de compartir información por medio de la nube, las redes sociales, la interconexión entre redes y la conexión de dispositivos, han permitido explorar vulnerabilidades en los sistemas lo cual ha conllevado a grandes amenazas para las infraestructuras tecnológicas y su información.

Hoy en día la información se toma como aquel activo esencial para las actividades de la organización, y en consecuencia, necesita protección adecuada, esta puede existir de diversas formas, puede estar impresa o escrita en papel, almacenada electrónicamente, transmitida por medio de correo electrónico o por cualquier otro medio electrónico.

A continuación, se muestran las temáticas relevantes para el desarrollo de la investigación:

4.1 SEGURIDAD INFORMÁTICA

Según la NIST, la seguridad informática es la protección otorgada a un sistema de información con el propósito de preservar la integridad, disponibilidad y confidencialidad de los recursos del sistema informático incluyendo software, hardware, firmware, información y telecomunicaciones.[2]

Es importante tener en cuenta que no se puede dar por entendido que un plan de seguridad es para mantener los sistemas en un 100% seguros, en tanto que, la seguridad absoluta no se puede asegurar, los riesgos siempre están presentes independiente de las medidas que se tengan, por lo cual se habla de mitigación de los riesgos en diferentes niveles de seguridad.[3]

---

[2] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY [Instituto Nacional De Estándares y Tecnología]. SPECIAL PUBLICACION 800-12: AN INTRODUCTION TO COMPUTER SECURITY: THE NIST HANBOOK [en línea]. [Consultado 25 Oct, 2014]. Disponible en <http://csrc.nist.gov/publications/nistpubs/800-12/800-12-html/chapter1.html>

[3] ASOCIACIÓN ESPAÑOLA PARA LA CALIDAD (AEC). Seguridad de la información. Centro Conocimiento. Madrid. España. [Consultado 20 Oct, 2014]. Disponible en: http://www.aec.es/web/guest/centro-conocimiento/seguridad-de-la-informacion

4.1.1 Objetivo. El objetivo principal es mantener salvaguardados los activos más importantes, preservando los tres pilares o principios, tales como son, la confidencialidad, integridad y disponibilidad de los recursos y activos mediante diversos controles, para ello, estos se deben establecer, implementar y monitorear asegurando así que se cumplan los objetivos planteados de seguridad alineados a la organización.

4.1.2 Amenazas. Es todo aquello con lo que se puede atentar contra la seguridad, bien sean acciones o elementos de los cuales se vea comprometida la integridad de los activos; dichas amenazas pueden surgir a partir de vulnerabilidades que suelen ser aprovechadas dentro de la organización, con el fin de obtener algún tipo de beneficio.

Dentro de las cuales se pueden encontrar:

4.1.2.1. Amenazas de factor humano: las cuales pueden ser causadas por los mismos usuarios de la entidad, por personas que trabajaron allí, curiosos y externos que quieren atacar en cuanto a información se refiere**.**

4.1.2.2. Amenazas de factor ambiental: De este tipo de amenazas podemos encontrar los desastres naturales, inundaciones, incendios entre otros que puedan alterar el continuo funcionamiento de la entidad.

4.1.2.3. Amenazas físicas y lógicas: las cuales se pueden producir por falla en la vida útil de los discos duros, servidores, interrupciones de energía y las más encontradas que son los virus los cuales han sido una de las principales amenazas para los sistemas ya que se propagan rápidamente y pueden ser introducidos con facilidad sin ser detectados.

Sin duda muchas organizaciones tienen conocimiento sobre las amenazas a las cuales se encuentran expuestas, pero por diferentes motivos no cuentan con los recursos para realizar y poner en operatividad planes que ayuden a mitigar este tipo de riesgos; por el contrario otras no cuentan con el conocimiento suficiente sobre la importancia de contar con diferentes estrategias en seguridad informática para la protección de su infraestructura, sin que esta resulte en pérdidas incalculables para la organización.

4.2 ACTIVO

Es todo aquello que tiene valor para la organización, por lo tanto este requiere ser protegido

4.3 ANÁLISIS DEL RIESGO

Identificación de vulnerabilidades que puedan ser explotadas, ocasionando un daño dentro de la organización.

4.4 IMPACTO

Es la medición de la consecuencia producida al ser materializada una amenaza

4.5 INCIDENTE DE SEGURIDAD

Cualquier evento real o sospechado en cuanto a la seguridad de sistemas informáticos o redes, en el acto de violar una política de seguridad explicita.

4.6 PROBABILIDAD

Es la posibilidad de que un hecho o incidente ocurra dentro de la organización.

4.7 RIESGO

Posibilidad de que se produzca un impacto, sobre un activo de la organización.

5. DIAGNÓSTICO

5.1 INDAGACIÓN INICIAL

En la indagación inicial se realizó un proceso de observación y una encuesta (véase Anexo A) a los Ingenieros del área de sistemas, como fuentes de información del estado de la organización con relación a la seguridad, en este proceso se detectó que la organización SECAB no cuenta con un plan de seguridad definido, en tanto que, no cuenta con procesos estructurados en cuanto al manejo de los sistemas de información, tratamiento del riesgo. Por tal razón, se inició el proceso de análisis con el fin de dar solución a esta carencia.

Para dicho propósito, fue necesario conocer la situación actual en cuanto a seguridad de la información se refiere y además saber cuáles son los activos críticos y/o sensibles con los que actualmente cuentan y si estos tienen una baja protección, en tanto que, representan un alto riesgo para la SECAB en caso de sufrir pérdida total o parcial. Este análisis permitió definir estrategias, ajustes y políticas para asegurar la protección de dichos activos.

6. ANÁLISIS Y GESTIÓN DEL RIESGO

En un proceso de análisis y gestión del riesgo podremos conocer una evaluación previa de aquellos riesgos con el fin de poder identificarlos y clasificarlos, dando así una implementación de controles.

A continuación se dará un análisis de forma cualitativa, con una probabilidad de que ocurra y el impacto que este pueda tener.

6.1 ANÁLISIS

6.1.1 Identificación del riesgo

6.1.1.1. Identificación y valoración de activos. Para realizar este tipo de identificación se accede directamente al inventario de activos actuales con los que cuentan en la organización y a la persona responsable de esta gestión. Tal como lo muestra el cuadro 1.

Después de realizar dicha consulta, se procede a realizar la valoración de acuerdo con la norma ISO-27005 anexo B, de la serie ISO 27000

Cuadro 1. Activos de soporte

Activos de soporte	
Tipo	**Descripción**
Hardware	Pc's, servidores, portátiles, impresoras, Discos externos, Cd's.
Software	Sistema operativo, sistemas de información.
Red	switch, Modem
Personal	Personas que actúan e interactúan dentro de la organización.
Sitio	Instalaciones
Servicios esenciales	Telefonía, servicios públicos
Fuente: La Autora	

A continuación se denotan los criterios y escalas que se tuvieron en cuenta para dar valor a los activos especificados.

Cuadro 2. Criterios y escala

Criterios	Escala
Problemas en el desempeño del negocio	Bajo
Incumplimientos contractuales	
Interrupción en la prestación del servicio	Medio
Costos financieros adicionales para emergencias	
Pérdida de activos físicos	
Pérdida de competitividad	Alto
Daños materiales	
Pérdidas financieras	
Pérdida de información física y digital	Muy Alta
Fuente: La Autora	

Después de realizar los criterios anteriores, se procede a hacer un análisis completo sobre la importancia y la valoración de los activos actuales, lo cual se expresa en el cuadro 3

Cuadro 3. Valoración de activos

Tipo de activo	Activo	Valor
Hardware	Equipos de Escritorio	Medio
	Portátiles	Bajo
	Impresoras	Bajo
	Discos externos	Muy alto
	Cd´s	Medio
	Servidores	Muy alto
Software	Sistemas operativos para servidores	Alto
	Sistema operativo para equipos	Bajo
	Licenciamiento	Medio
	Sistemas de información (contable, recursos humanos, archivo)	Muy alto
Red	Switch	Alto
	Modem	Alto
Personal	Administradores de los sistemas	Medio
	Encargados de copias de seguridad	Medio
	Personal de recursos humanos	Medio
	Personal de financiera	Medio
	Personal Externo	Medio
Sitio	Edificio	Bajo
	Cuarto de servidores	Alto
	Servicios esenciales	Alto
Organización	Información	Muy alto
	Procesos	Medio
Fuente: La Autora		

6.1.1.2 Identificación de las amenazas. Existen diferentes tipos de amenazas, las cuales explotan vulnerabilidades existentes dentro de la organización, provocando incidentes que pueden ocasionar daños en los activos.

En donde el origen puede ser A (accidental), D (deliberado), E (ambiental)

Cuadro 4. Identificación de amenazas

Tipo	Amenazas	Origen
Daño Físico	Corrosión, polvo, accidentes, daños por inundaciones, destrucción de equipos.	A,D,E
Fenómenos Naturales	Sismos, inundaciones, climáticos, volcánicos.	E
Pérdida de los servicios esenciales	Fallas en el servicio de energía	A,D,E
	fallas en los equipos de telecomunicaciones	A,D
	fallas en los suministros de agua	A,D
Fallas técnicas	Fallas en los equipos, mal funcionamiento del software	A
	Saturación en los sistemas de información, incumplimiento del mantenimiento en los sistemas de información	A,D
Compromiso de la información	Espionaje Remoto, robo de equipos, robo de documentos o medios, manipulación con hardware	D
	Manipulación con software, divulgación	A,D

Cuadro 4. (Continuación)

Tipo	Amenazas	Origen
Acciones no autorizadas	Usos no autorizados de equipos, copia fraudulenta del software, adulteración de la información	A
	Uso de software falso	A,D
Compromiso de las funciones	Error en el uso, falsificación de derechos	A
	Abuso de derechos	A,D
Fuente: La Autora		

6.1.1.3 Identificación de Vulnerabilidades. A continuación se presenta el cuadro 5 de evaluación de las vulnerabilidades frente a los activos y amenazas, obteniendo así una determinación de diversos escenarios en cuanto a incidentes.

Cuadro 5. Identificación de vulnerabilidades

Tipo de activo	Vulnerabilidades	Amenazas
Hardware	Susceptibilidad a las variaciones de energía	Fallas y/o daño del medio por problemas de energía
	Almacenamiento sin protección controlada	Robo de documentos o medios
	Copias no controladas	Robo de documentos o medios
	Falta de planes en cuanto a reemplazos	Daño físico por Corrosión, polvo, accidentes
	Usos inapropiados de los dispositivos tecnológicos	Funcionamiento incorrecto de los dispositivos

Cuadro 5. (Continuación)

Software	Falta de pruebas de auditoria	Abuso de derechos
	Falta de documentación	Error en el uso
	Software nuevo	Mal funcionamiento del software
	Falla en la producción de informes de gestión	Uso no autorizado del equipo
	Falta de control en las entradas físicas	Robo de documentos o medios
	Falta de copias de respaldos externas de la organización	Manipulación con software
	Usos y descargas no controladas de software	Manipulación con software
	Requerimientos no claros e incompletos a los desarrolladores	Mal funcionamiento del software
Red	No se realizan pruebas de envío y recepción de mensajes	Espionaje remoto
	Falla en la conexión de cables	Falla de equipo de telecomunicaciones
	Conexiones de red pública sin protección controlada	Uso no autorizado de equipo
	Falla del canal principal	Falla de las comunicaciones internas y externas
	Transferencia de contraseñas	Espionaje remoto

Cuadro 5. (Continuación)

Tipo de activo	**Vulnerabilidades**	**Amenazas**
Personal	Falta de capacitación en seguridad	Error en el uso
	Falta de mecanismos de monitoreo	Procesamiento ilegal de datos
	Falta de supervisión al personal externo	Robo de documentos o medios
	Falta de capacitación para el uso de software y hardware	Erro en el uso
	Falta de políticas para el adecuado uso de las tecnologías	Usos no autorizados
Sitio	Control físico inestable al acceso al cuarto de servidores	Destrucción de equipos
	Suministros de energías inestables en el edificio	Perdida del suministro de energía
Organización	Falta de procedimientos para registros y retiros de usuarios	Abuso de los derechos
	Falta de monitoreo de los recursos en donde se procesa la información	Abuso de los derechos
	Falta de auditorías internas	Abuso de los derechos
	Falta de planes de continuidad	Falla de equipos
	Falta de bitácoras para controles	Error en el uso
	Falta de manuales de usuario para los S.I.	Error en el uso
	Falta de procesos disciplinarios	Hurto de equipo y/o información
	Falta de monitoreo para detectar problemas de seguridad	Hurto de documento o medios
Fuente: La Autora		

6.2 EVALUACIÓN DEL RIESGO

Para realizar la evaluación de Riesgo, se procede a plasmar la cuantificación de una escala de probabilidad en cuanto a la ocurrencia y al impacto, medidas de la siguiente manera (ver cuadro 6):

Cuadro 6. Probabilidad de ocurrencia

Probabilidad de ocurrencia		
Valor	**Categoría**	**Descripción**
1	Improbable	Una vez en 20 años
2	Poco probable	Ocurre una vez en los últimos 10 años
3	Probable	Ocurre una vez en los últimos 5 años
4	Muy probable	Ocurre una vez en el último año
5	Frecuente	Ocurre varias veces en el año
Fuente: La Autora		

A continuación se relaciona la manera en cómo se evalúa el impacto y su categorización.

Cuadro 7. Impacto del riesgo

Impacto						
Cualitativa		puede obstruir en la operación, pero no tienen trascendencia	Dificulta la operatividad, pero con aplicación de medidas no se descontinua el objetivo	Afecta operatividad, sin alteración	Obstruye operatividad	Perturba la operatividad de manera grave, imposibilitando su continuidad
Monetaria		los sobre costos no superan el 1%	los sobrecostos no superan el 10%	el impacto sobre el valor esta entre el 10% y el 15%	Incrementa el valor entre el 15% y el 30%	Impacto sobre el valor está por encima del 30%
Categoría	**Valoración**	Sin Impacto	Bajo	Medio	Alto	Muy Alto
		1	2	3	4	5
Fuente: La Autora						

Para cada Riesgo se deben sumar las valoraciones de probabilidad e impacto, para obtener la valoración total del Riesgo como se observa en el cuadro 8.

Cuadro 8. Valoración del riesgo

Probabilidad	**Impacto**				
	Sin Impacto (1)	Bajo(2)	Medio (3)	Alto (4)	Muy Alto (5)
Improbable (1)	1	2	3	4	5
Poco Probable (2)	2	4	6	8	10
Probable (3)	3	6	9	12	15
Muy Probable (4)	4	8	12	16	20
Frecuente (5)	5	10	15	20	25

Fuente: La Autora

Luego de realizar una valoración sobre el enfrentamiento del riesgo, este va a permitir que se establezcan categorías a cada una de estas valoraciones que se realizaron, para asignar un nivel de aceptación dentro de la organización. Para cada Riesgo se deben sumar las valoraciones de probabilidad e impacto, para obtener la valoración total del Riesgo (ver cuadro 9)

Cuadro 9. Categorías y valor del riesgo

Categoría	**Valoración del Riesgo**
Aceptable	1 - 4
Moderado	5 - 14
Inaceptable	15 - 25

Fuente: La Autora

A continuación se realiza la asignación de matriz de riesgo (cuadro 10 Y 11), en donde se encontrará la clasificación, el riesgo determinado con probabilidad e impacto que se obtiene para que con ello se pueda dar una valoración al riesgo, dando así algunas acciones que no permitan la ejecución del riesgo, mitigándolo.

Cuadro 10. Matriz de riesgo

Tipo de activo	Activo	Impacto	Vulnerabilidad	Amenaza	Probabilidad de ocurrencia	Riesgo (bruto)
Hardware	Servidor Página Web	5	Susceptibilidad a las variaciones de energía. Almacenamiento sin protección controlada. Falta de planes en cuanto a reemplazos.	Fallas y/o daño del medio por problemas de energía. Robo de documentos o medios. Daño físico por Corrosión, polvo, accidentes.	4	20
	Servidor Financiera	5			4	20
	Servidor Dominio	5			4	20
	Servidor Base de Datos	5			4	20
	Servidor Contabilidad	5			4	20
	Equipos De Escritorio	3	Usos inapropiados de los dispositivos tecnológicos. Falta de planes en cuanto a reemplazos	Funcionamiento incorrecto de los dispositivos. Daño físico por Corrosión, polvo, accidentes.	2	6
	Equipos Portátiles	2			2	4
	Impresoras	2			2	4
	Discos Externos (Backups)	5	Almacenamiento sin protección controlada	Robo de documentos o medios	4	20
	Copias de Informes en Cd´s	3			4	12

Cuadro 10. (Continuación)

Tipo de activo	Activo	Impacto	Vulnerabilidad	Amenaza	Probabilidad de ocurrencia	Riesgo (bruto)
Software	Sistemas Operativos (equipos de escritorio)	2	Falta de pruebas de auditoria. Usos y descargas no controladas de software	Abuso de derechos. Manipulación con software.	2	4
	Sistema Operativo de Servidores	4			4	16
	Saic	5	Falta de documentación. Falla en la producción de informes de gestión. Falta de copias de respaldos externas de la organización.	Error en el uso. Uso no autorizado del equipo. Manipulación con software. Mal funcionamiento del software.	4	20
	Seven	5			4	20
	Kactus	5			4	20
	Docuware	5			4	20
Red	switch	4	Falla en la conexión de cables. Falla del canal principal. Transferencia de contraseñas. Conexiones de red pública sin protección controlada.	Uso no autorizado de equipo. Falla de las comunicaciones internas y externas. Espionaje remoto	4	16
	Modem	2			4	16
Personal	Administradores	3	Falta de capacitación en seguridad. Falta de mecanismos de monitoreo. Falta de capacitación para el uso de software y hardware	Error en el uso. Procesamiento ilegal de datos. Usos no autorizados.	3	9
	Usuarios Internos (encargados de copias, personal de R.H, personal financiera)	3			3	9
	Usuarios externos	3	Falta de supervisión al personal externo	Robo de documentos o medios	3	9

Cuadro 10. (Continuación)

Tipo de activo	Activo	Impacto	Vulnerabilidad	Amenaza	Probabilidad de ocurrencia	Riesgo (bruto)
Sitio	Instalaciones	4	Control físico inestable al acceso al cuarto de servidores. Suministros de energías inestables en el edificio	Destrucción de equipos. Perdida del suministro de energía en las oficinas.	4	16
	Servicios Esenciales	4			4	16
Organización	Información	5	Falta de monitoreo de los recursos en donde se procesa la información. Falta de bitácoras para controles. Falta de mecanismos de monitoreo para detectar problemas de seguridad	Hurto de documento o medios. Abuso de los derechos. Error en el uso	5	25
	Procesos	3	Falta de procedimientos para registros y retiros de usuarios. Falta de auditorías internas. Falta de auditorías internas. Falta de manuales de usuario para los sistemas de información. Falta de procesos disciplinarios en caso de incidentes de seguridad	Abuso de los derechos. Error en el uso. Hurto de equipo y/o información	4	12
Fuente: La Autora						

Tras la elaboración de la Matriz que da como resultado un Riesgo (bruto), se va a catalogar el nivel de aceptación del riesgo dentro de la SECAB, los cuales se darán de la siguiente manera:

Cuadro 11. Aceptación del riesgo

Activo	Vulnerabilidad	Amenaza	Riesgo (bruto)	Nivel de aceptación
Servidor Página Web	Susceptibilidad a las variaciones de energía. Almacenamiento sin protección controlada. Falta de planes en cuanto a reemplazos.	Fallas y/o daño del medio por problemas de energía. Robo de documentos o medios. Daño físico por Corrosión, polvo, accidentes.	20	Inaceptable
Servidor Financiera			20	Inaceptable
Servidor Dominio			20	Inaceptable
Servidor Base de Datos			20	Inaceptable
Servidor Contabilidad			20	Inaceptable
Equipos De Escritorio	Usos inapropiados de los dispositivos tecnológicos. Falta de planes en cuanto a reemplazos	Funcionamiento incorrecto de los dispositivos. Daño físico por Corrosión, polvo, accidentes.	6	Moderado
Equipos Portátiles			4	Aceptable
Impresoras			4	Aceptable
Discos Externos (Backups)	Almacenamiento sin protección controlada	Robo de documentos o medios	20	Inaceptable
Copias de Informes en Cd´s			12	Moderado
Sistemas Operativos (equipos de escritorio)	Falta de pruebas de auditoria. Usos y descargas no controladas de software	Abuso de derechos. Manipulación con software.	4	Aceptable
Sistema Operativo de Servidores			16	Inaceptable
Saic	Falta de documentación. Falla en la producción de informes de gestión. Falta de copias de respaldos externas de la organización.	Error en el uso. Uso no autorizado del equipo. Manipulación con software. Mal funcionamiento del software.	20	Inaceptable
Seven			20	Inaceptable
Kactus			20	Inaceptable
Docuware			20	Inaceptable

Cuadro 11. (Continuación)

Activo	Vulnerabilidad	Amenaza	Riesgo (bruto)	Nivel de aceptación
Switch	Falla en la conexión de cables. Falla del canal principal. Transferencia de contraseñas. Conexiones de red pública sin protección controlada.	Uso no autorizado de equipo. Falla de las comunicaciones internas y externas. Espionaje remoto	16	Inaceptable
Modem			16	Inaceptable
Administradores	Falta de capacitación en seguridad. Falta de mecanismos de monitoreo. Falta de capacitación para el uso de software y hardware	Error en el uso. Procesamiento ilegal de datos. Usos no autorizados.	9	Moderado
Usuarios Internos (encargados de copias, personal de R.H, personal financiera)			9	Moderado
Usuarios externos	Falta de supervisión al personal externo	Robo de documentos o medios	9	Moderado
Instalaciones	Control físico inestable al acceso al cuarto de servidores. Suministros de energías inestables en el edificio	Destrucción de equipos. Perdida del suministro de energía en las oficinas.	16	Inaceptable
Servicios Esenciales			16	Inaceptable

Cuadro 11. (Continuación)

Activo	Vulnerabilidad	Amenaza	Riesgo (bruto)	Nivel de aceptación
Información	Falta de monitoreo de los recursos en donde se procesa la información. Falta de bitácoras para controles. Falta de mecanismos de monitoreo para detectar problemas de seguridad	Hurto de documento o medios. Abuso de los derechos. Error en el uso	25	Inaceptable
Procesos	Falta de procedimientos para registros y retiros de usuarios. Falta de auditorías internas. Falta de auditorías internas. Falta de manuales de usuario para los sistemas de información. Falta de procesos disciplinarios en caso de incidentes de seguridad	Abuso de los derechos. Error en el uso. Hurto de equipo y/o información	12	Moderado
Fuente: La Autora				

6.3 TRATAMIENTO DEL RIESGO

Para cada uno de los riesgos identificados anteriormente en su evaluación, se deben tomar decisiones en cuanto al control pertinente que se tomará para ellos, teniendo en cuenta los siguientes parámetros:

- Aplicación de los controles apropiados para reducir los riesgos.
- Aceptación objetiva y con conocimiento de los riesgos, siempre y cuando ellos satisfagan la política de la organización y sus criterios para la aceptación del mismo.
- Evitación de los riesgos al no permitir acciones que pudieran hacer que éstos se presentaran.
- Transferencia de riesgos asociados a otras partes.

Cuadro 12. Controles

Activo	Vulnerabilidad	Amenaza	Nivel de aceptación	Control
Servidor Página Web	Susceptibilidad a las variaciones de energía. Almacenamiento sin protección controlada. Falta de planes en cuanto a reemplazos.	Fallas y/o daño del medio por problemas de energía. Robo de documentos o medios. Daño físico por Corrosión, polvo, accidentes.	Inaceptable	Mantenimientos periódicos a los servidores y UPS. Check list de funcionamiento. Bitácoras de acceso al centro de servidores. Equipos en stock disponibles para ser reemplazados frente a cualquier eventualidad.
Servidor Financiera			Inaceptable	
Servidor Dominio			Inaceptable	
Servidor Base de Datos			Inaceptable	
Servidor Contabilidad			Inaceptable	
Equipos De Escritorio	Usos inapropiados de los dispositivos tecnológicos. Falta de planes en cuanto a reemplazos. Hardware obsoleto.	Funcionamiento incorrecto de los dispositivos. Daño físico por Corrosión, polvo, accidentes.	Moderado	Capacitación de usuarios para uso de los medios tecnológicos. Socialización de las políticas de uso. Stock o actualización de hardware.
Equipos Portátiles			Aceptable	
Impresoras			Aceptable	
Discos Externos (Backups)	Información sin protección. Almacenamiento sin protección controlada. Falta de procesos de custodia de los medios	Visibilidad de información sensible. Robo o pérdida de documentos o medios.	Inaceptable	Encriptación de la información. Asignación de lugar estratégico seguro. Bitácoras o formatos que permitan identificar custodia de medios.
Copias de Informes en Cd´s			Moderado	

Cuadro 12. (Continuación)

Activo	Vulnerabilidad	Amenaza	Nivel de aceptación	Control
Sistemas Operativos (equipos de escritorio)	Falta de auditoria. Software obsoleto. Usos y descargas no controladas de software. Falta de planeación para instalación de parches. Acceso no autorizado	Abuso de derechos. Daño de sistema causado por software malicioso Manipulación con software. Penetración de sistema operativo	Aceptable	Programación de auditorías internas. Planes para actualizar el sistema operativo Asignación de permisos por usuario. Ambientes de pruebas para verificación de funcionalidad de los parches del sistema. Identificación y autenticación de usuarios.
Sistema Operativo de Servidores			Inaceptable	
Saic	Falta de documentación. Falla en la producción de informes de gestión. Falta de copias de respaldos externas de la organización.	Error en el uso. Uso no autorizado del equipo. Manipulación con software. Mal funcionamiento del software.	Inaceptable	Actualización de aplicaciones y adquisición del software con manuales de instalación. Asignación de roles por usuarios. Backups realizados por terceros. Implementación de manuales de funcionamiento para los usuarios.
Seven			Inaceptable	
Kactus			Inaceptable	
Docuware			Inaceptable	
switch	Falla en la conexión de cables. Denegación de Servicio. Falla del canal principal. Transferencia de contraseñas. Conexiones de red pública sin protección controlada.	Uso no autorizado de equipo. Acceso y administración a red interna Falla de las comunicaciones internas y externas. Espionaje	Inaceptable	Canal alterno de comunicación. Establecer seguridad perimetral. Monitoreo de red. Control sobre la protección de Red. Autenticación para conexión
Router			Moderado	

Cuadro 12. (Continuación)

Activo	Vulnerabilidad	Amenaza	Nivel de aceptación	Control
Administradores	Falta de capacitación en seguridad. Falta de capacitación para el uso de software y hardware	Error en el uso. Procesamiento ilegal de datos. Usos no autorizados.	Moderado	Toma de capacitaciones on-line o presenciales sobre temas de seguridad
Usuarios Internos (encargados de copias, personal de R.H, personal financiera)			Moderado	Capacitaciones internas para instruir al usuario (campañas, actividades, ect) Instrucciones a los usuarios por parte del personal de tecnología para el uso de medios tecnológicos
Usuarios externos	Falta de supervisión al personal externo	Robo de documentos o medios	Moderado	Supervisión de actividades
Instalaciones	Control físico inestable al acceso al cuarto de servidores. Suministros de energías inestables en el edificio	Destrucción de equipos. Perdida del suministro de energía en las oficinas.	Inaceptable	Bitácora de ingreso. Control adicional físico para el acceso como Biométricos, usos de tarjetas magnéticas entre otros que puedan ser de consideración.
Servicios Esenciales			Inaceptable	UPS adicional. Mantenimiento y revisiones periódicas a las UPS.

Cuadro 12. (Continuación)

Activo	Vulnerabilidad	Amenaza	Nivel de aceptación	Control
Información	Falta de monitoreo de los recursos en donde se procesa la información. Falta de bitácoras para controles. Falta de mecanismos de monitoreo para detectar problemas de seguridad	Hurto de documento o medios. Abuso de los derechos. Error en el uso	Inaceptable	Fijar controles en cuanto a restricciones de puertos, filtros para el envió de información a correos externos. Implementación de Bitácoras para documentos físicos.
Procesos	Falta de procedimientos para registros y retiros de usuarios. Falta de auditorías internas. Falta de manuales de usuario para los sistemas de información. Falta de procesos disciplinarios en caso de incidentes de seguridad	Abuso de los derechos. Error en el uso. Hurto de equipo y/o información	Moderado	Establecer procesos definidos y darlos a conocer dentro del organismo. Planeación de auditorías internas. Definiciones de sanciones frente a fallas disciplinarias. Documentar todos los procedimientos, requerimientos, incidentes y responsabilidades
Fuente: La Autora				

7. POLÍTICAS DE SEGURIDAD[4]

7.1 POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

Con el siguiente documento se pretende brindar orientaciones y apoyo en materia de la seguridad de la información, teniendo en cuenta las necesidades, requisitos y reglamentos de la SECAB.

Es necesario que las directivas establezcan un direccionamiento claro de políticas y demuestren su apoyo y compromiso con la organización.

7.1.1 Alcance: Es importante que las políticas y los estándares de seguridad sean observados de manera obligatoria por todos los funcionarios, contratistas u otras partes que tengan relación con la SECAB, esto con el fin de preservar el buen uso de los servicios tecnológicos y de información que se encuentren dentro de la organización.

7.1.1 Objetivos:

- Proteger los recursos tecnológicos y la información de la SECAB, frente a las diferentes amenazas que se puedan encontrar de manera interna o externa.

- Preservar de manera actualizada y operativa las políticas de seguridad establecidas, asegurando así su eficiencia y validez dentro de la organización.

- Prevenir incidentes de seguridad de la información en la SECAB.

[4] El parámetro con base al cual se realizó el presente documento fue de la serie ISO 27000. Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC). Código de práctica para la gestión de la seguridad de la información. Bogotá. NTC ISO/IE 27002. 2007. Disponible en: http://www.iso27002.es/

7.2. DOCUMENTO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Se recomienda tener en cuenta los siguientes aspectos para la elaboración del documento de políticas de seguridad de la información, el cual, una vez elaborado, será revisado y en dado caso aprobado por la directiva de la SECAB.

Los aspectos en mención son:

- **Acuerdos de confidencialidad:** como acuerdo inicial de contratación, es menester que los funcionarios, contratistas o terceros sin importar su nivel de jerarquía institucional dentro de la SECAB, firmen un acuerdo de confidencialidad, lo cual quedará como constancia de la aceptación dentro de su contrato.

- **Uso adecuado de los activos:** resulta pertinente establecer normas de acceso y restricción a los documentos físicos y digitales, de acuerdo con las competencias y necesidades de los usuarios, previamente definidas por los jefes de cada área.

- **Acceso a Internet:** siendo esta una herramienta de trabajo que permite acceso a múltiples páginas relacionadas directa o indirectamente con la organización, se sugiere realizar un control y monitoreo, en donde:

    - No se permita el acceso a páginas que relacionen temas pornográficos, hacking, drogas y/o cualquier otro que vaya contra la moral, ética o políticas que se establezcan.
    - Bloqueo para descargas, instalaciones y usos de juegos, películas u otro tipo de software libre o ejecutable que atente contra la propiedad intelectual de sus autores y/o la integridad, disponibilidad y confidencialidad de los activos tecnológicos y de información.
    - Realizar monitoreo permanente de páginas a las cuales han accedido los usuarios que hayan hecho uso de la red interna. Por parte del responsable asignado.
    - Los accesos de navegación no serán usados para prácticas ilícitas o mal intencionadas que atenten contra personas internas y externas a la SECAB.
    - Cada usuario es responsable del uso adecuado al recurso proporcionado, el cual se debe realizar de manera ética y responsable sin afectar la protección de la información, el buen nombre y demás consideraciones del organismo.

- **Correo Electrónico:** Es recomendable que los funcionarios y contratistas a los cuales se les asigne una cuenta de correo electrónico institucional, tengan en cuenta lo siguiente:

    - Las cuentas de correo solo serán usadas para el cumplimiento de las funciones asignadas en la SECAB, si por algún motivo es utilizada para uso personal este será de manera ética y responsable del usuario.
    - No se permitirá el uso del correo para envió de cadenas, mensajes con contenido racista, sexista, religioso, publicitario que no sea corporativo o cualquier tipo de mensaje que atente contra la dignidad y moral de las personas, esto se medirá por medio de monitorio de contenido.
    - El uso de la dirección de correo electrónico no podrá ser utilizada como referencia en redes sociales o cualquier sitio que no esté relacionada con las actividades laborales.
    - Si se realiza envió masivos de mensajes publicitarios, estos deberán contar con la aprobación del área de comunicaciones y enviados desde la cuenta genérica institucional del área.

- **Recursos Tecnológicos:** se sugiere que el uso adecuado de los recursos tecnológicos que hayan sido asignados, cuente con la siguiente protección:

    - Si se requiere instalación de software, este contará con una autorización directa del jefe de área y la instalación la realizará el área de sistemas.
    - De ser necesario realizar movimientos de equipos de cómputo o manipulación de cables, protectores de pantalla y demás recursos establecidos, esta labor solo será realizada por el área de sistemas.
    - Si se requiere del uso de la red inalámbrica, se contactará al área de sistemas para la configuración de la misma.
    - Si se desea realizar conexión remota a recursos internos, se contará con la autorización escrita por parte del jefe encargado del área y aprobación directa del oficial de seguridad.

- **Seguridad física y del entorno:** Es importante contar con las implementaciones de mecanismos que permitan controlar los accesos físicos a las instalaciones y demás que detecten inconsistencias en el entorno que se encuentren los activos tecnológicos y de información. Esto con el fin de evitar daños, pérdida, robo o cualquier amenaza que se pueda presentar.

- **Protección contra software malicioso:** Dentro de la organización, resulta necesario, poner en funcionamiento herramientas como antivirus, antispam u otras que se consideren puedan ser preventivas de protección, para evitar

posibles fallas por la ejecución y propagación de códigos maliciosos en la red institucional.

- **Control de acceso:** Se sugiere que todos los servicios institucionales que se encuentren a disposición de los usuarios, tales como sistemas de información, uso de red y recursos compartidos de información, se encuentren controlados por acceso lógicos los cuales se basarán en roles de acuerdo a la necesidad de cada usuario, identificándose con un ID y password.

- **Cumplimiento de políticas:** Es importante establecer tiempos de verificación del cumplimiento de las políticas por parte de los funcionarios y contratistas sin importar su nivel de jerarquía, contemplando sanciones disciplinarias o laborales si se detecta el incumplimiento o violaciones a las políticas que se establezcan. Se pueden establecer reuniones con directivas en donde el oficial de seguridad presente informes sobre el monitoreo, incidentes y demás que se presenten, en los cuales se mida el comportamiento de todos los usuarios hacia las políticas.

7.2.1 Revisión de la política de seguridad de la información. Las políticas de seguridad planteadas y aprobadas por la Secretaria Ejecutiva de la SECAB, podrían ser revisadas con una periodicidad no mayor a 6 meses o en su defecto si se producen cambios de alta relevancia, garantizando así su aplicabilidad, suficiencia y eficacia; esto realizado por la persona encargada de seguridad y las partes interesadas dentro de la organización.

Dentro de las reuniones para la revisión del documento de las políticas se propone tener en cuenta los siguientes ítems a incluir en la toma de decisiones.

- Desempeño y cumplimiento de las políticas de seguridad.
- Tener en cuenta si los cambios pueden afectar el enfoque de la SECAB (cambios en el entorno, disponibilidad de recursos)
- Incidentes de seguridad que se hayan presentado.
- Mejoras en la asignación de recursos y responsabilidades.

Toda vez sea revisado y/o modificado el documento de políticas, deberá quedar constancia sobre la persona y el tipo de acción que se ejerció, posterior a ello deberá contar con la aprobación de la Secretaria Ejecutiva.

8. ORGANIZACIÓN DE LA SEGURIDAD

8.1 ORGANIZACIÓN INTERNA

8.1.1 Compromiso de la dirección con la seguridad de la información. Se recomienda que la Secretaría ejecutiva, en su calidad de directiva, apoye de manera efectiva la seguridad de la información, en cuanto al conocimiento de funciones y las respectivas responsabilidades que se le encuentren asignadas, demostrando con esto un compromiso.

En donde tal compromiso se verá visualizado por medio de:

- Aprobación del documento en donde se encuentran las políticas de seguridad para su aplicación y ejecución.
- Revisiones en cuanto a la eficacia en las implementaciones de las políticas de seguridad.
- Velación por el cumplimiento de las políticas de seguridad.
- Aprobación de modificaciones, funciones y responsabilidades directas dentro del marco de la seguridad, dentro de la SECAB.
- Realizar otro tipo de actividad a fines pertinentes que sean concernientes con la seguridad de la información.
- Apoyar, efectuar y hacer cumplir las actividades e iniciativas de seguridad que se den dentro de la organización.

8.1.2 Coordinación de la seguridad de la información. Se propone que la SECAB cuente con un oficial de seguridad de la información, quien deberá asumir diferentes tareas y roles de responsabilidad, tales como:

- Diferentes tipos de entrenamientos didácticos para la capacitación de los funcionarios, contratistas o terceros.
- Capacitarse en los temas pertinentes, para estar actualizado con respecto a las amenazas y vulnerabilidades existentes, las cuales son de constante cambio.
- Proveer lineamientos para el control de acceso y modificación de privilegios en los sistemas de información.
- Minimizar perdidas en los activos de información dentro de la organización.
- Actualización de las políticas y procedimientos que se hayan definido.
- Seleccionar, evaluar e implementar herramientas que promuevan y faciliten las diferentes labores en la seguridad de la información.

- Fomentar dentro de la organización la cultura y educación en cuanto a temas relacionados con la seguridad de la información, implementando.

8.1.3 Asignación de responsabilidades para la seguridad de la información. Todo aquel funcionario que desempeñe cargos de relevancia (jefes de áreas), necesita coordinar sus respectivas actividades con el Responsable de la Seguridad informática, esto con el propósito de cumplir y consolidar los aspectos de las políticas internas.

Asegurando en sus respectivas áreas las responsabilidades de:

- Garantizar que las actividades de seguridad sean aplicadas en conformidad con las políticas establecidas.
- Aprobar procesos y técnicas de seguridad.
- Reconocer amenazas a las que se encuentra expuesta la información y el procesamiento de la misma.
- Promover la educación y concienciación sobre la seguridad.
- Evaluar controles e informes.

Cabe mencionar que, en todos los casos, él responsable puede delegar sus funciones al personal que se considera idóneo a su cargo, pero este sigue asumiendo la responsabilidad sobre el cumplimiento de las mismas.

En el siguiente listado, se sugieren unas pautas que pueden ayudar a reconocer las responsabilidades de las siguientes áreas:

- **Recursos Humanos:** el personal encargado de dicha área, puede notificar al personal contratado e ingresante, el cumplimiento de las políticas y procedimientos, posterior de ello notificar al área de sistemas el ingreso de dicho funcionario para su respectiva asignación de usuarios y capacitaciones correspondientes.
- **Sistemas:** el responsable del área de sistemas, asegurará el cumplimiento de todos los requerimientos establecidos para el diseño, adquisición y mantenimiento de los recursos tecnológicos de la SECAB.
- **Jurídica:** esta área velará por la gestión del cumplimiento de las políticas dentro de los contratos, acuerdos y/o documentos oficiales que la SECAB tenga con funcionarios y/o terceros. También asesorará al área que lo requiera en materia de incumplimientos legales en la parte de la seguridad.
- **Administrativa y Financiera:** los responsables apoyarán activamente las decisiones en cuanto a la adquisición de elementos (software, hardware, físicos de protección en la infraestructura) que permitan ejercer la continuidad

de la seguridad, la parte encargada de contratos incluirá dentro de los documentos oficiales a la contratación la obligatoriedad del cumplimiento de las políticas de seguridad y sus procedimientos relacionados.

- **Áreas Misionales:** respetar y hacer cumplir a sus subordinados las políticas de seguridad informando sobre incidentes o cualquier anomalía que se presente dentro del área que de incumplimiento a cualquiera de ellas.

8.1.4 Proceso de autorización para los servicios de procesamiento de información. Si se desea adquirir una nueva herramienta en beneficio de los controles para la seguridad, se recomienda que cuente con los siguientes lineamientos:

- La parte de sistemas, determinará su compatibilidad en cuanto software y hardware.
- El oficial de seguridad se involucrará para decidir si dicha herramienta cumple finalmente con los parámetros de seguridad requeridos y su propósito dentro de la SECAB.
- La Secretaria Ejecutiva recibirá un informe detallado sobre el propósito y el uso de dicha herramienta; determinando así su aprobación para la adquisición de la misma.

8.1.5 Acuerdos sobre confidencialidad. Se recomienda adaptar e incluir acuerdos y/o cláusulas de confidencialidad que permitan proteger adecuadamente la información clasificada y derechos de autor, que contemplen la devolución de aquellos activos utilizados por los funcionarios y/o terceros al finalizar su vínculo laboral.

Las siguientes cláusulas podrían ser descritas por contrato

- **Información Confidencial:** La parte no divulgará la información catalogada como confidencial (siendo esta: informes financieros, contables, baremos de contribución, informes jurídicos, banco de imágenes, patrimonio intelectual en este caso denominado publicaciones e información tecnológica) por ningún medio; llámese este verbal, escrito (correo electrónico, medios extraíbles), impreso en papel y/o en cualquier método de divulgación
- **Confidencialidad:** La parte no comunicará a persona o entidad (pública, internacional o privada) alguna, la información reservada que llegue a su conocimiento en razón a la ejecución del presente contrato. Esta disposición seguirá vigente después de la terminación del presente contrato.

- **Derechos de Autor:** Si durante el desarrollo del objeto del presente contrato se generan creaciones o desarrollos que deban ser protegidas por la legislación vigente en materia de derechos de autor, a la parte se le reconocerán los derechos morales a los que haya lugar por la autoría, y a la SECAB se le reconocerá la titularidad única sobre los derechos patrimoniales que se generen, los cuales se transfieren sin limitación temporal ni territorial, de conformidad con lo establecido por los Artículos 28 y 30 de la ley 1450 del 2011.
- **Incumplimiento:** El incumplimiento de las obligaciones de confidencialidad por la parte, facultará a la SECAB a reclamar por la vía legal que esta estime procedente, indemnizaciones por los daños y perjuicios ocasionados.

8.1.6 Contacto con las autoridades y grupos de interés especiales. En identificación de las autoridades pertinentes, se establece la posible forma de tomar contacto con ellas, reportando oportunamente incidentes de seguridad, o sospechas sobre incumplimiento de la ley.

Cada área relacionada cuenta con todos los datos pertinentes al contacto de comunicación directo.

- **Con relación a la continuidad:** electricidad, agua; se dará por informada al área administrativa.
- **Con relación a las redes**: desde el área de sistemas se comunicará directamente el incidente al proveedor de red.
- **Incumplimiento de ley en cuanto a delitos informáticos:** el oficial de seguridad se contactará con el Centro Cibernético Policial, en donde podrá establecer el reporte del incidente (Hurto) presentado.

En cuanto a Grupos de Interés y organismos de apoyo se encuentran:

El oficial de seguridad podrá mejorar conocimientos en cuanto a mejores prácticas y estar actualizado con la información relacionada la seguridad a través de asesorías especializadas, intercambio de información acerca de nuevas tecnologías y amenazas; lo que le permitirá estar a la vanguardia para prevenir y generar oportunas alertas de ataques.

- **CIRTISI (Centro de Información y Respuesta Técnica a Incidentes de Seguridad Informática):** el oficial de seguridad, se apoyará en este grupo especializado para ayudar a ampliar información en materia de investigación a incidentes presentados, la SECAB por ser un organismo Intergubernamental podrá contar también con un apoyo a respuesta de incidentes.

- **COLCERT (Grupo de Respuesta a Emergencias Cibernéticas de Colombia)**

8.2 PARTES EXTERNAS

8.2.1 Identificación de los riesgos relacionados con las partes externas. Cuando exista la necesidad de dar acceso a partes externas (terceros) sobre la información y/o recursos de la SECAB, se sugiere que el oficial de seguridad informática y el propietario de la información y/o recurso, lleven a cabo una evaluación del riesgo, documentando los controles específicos, términos y condiciones para la conexión o acceso a la parte requerida.

Para ello se pueden tener en cuenta los siguientes aspectos, para otorgar el acceso

- El tipo de acceso y el recurso al cual se solicita acceso.
- Razón por la cual se solicita el acceso.

En donde el oficial de seguridad definirá:

- Control aplicable por la tercera parte.
- La afectación de dicho acceso en la seguridad de la organización.

Bajo ninguna circunstancia se dará acceso a las partes externas (terceros), sin antes garantizar que dicha parte es consciente de sus obligaciones y que acepta las responsabilidades que involucran dar acceso y procesamiento del recurso de la SECAB.

Cada parte bajo su objeto contractual, tendrá estipulado la cláusula de confidencialidad, posterior a ello se propone establecer los siguientes controles:

- Cumplimiento de las políticas de seguridad establecidas en la SECAB.
- Restricciones de copias de la información.

- Identificación única para el acceso permitido (usuario y contraseña)
- Monitoreo para detección de incidentes o violaciones de seguridad.
- Control de accesos y privilegios asignados.
- Capacitaciones en materia de seguridad.
- Control bajo software malicioso.

9. GESTIÓN DE ACTIVOS

9.1 RESPONSABILIDAD DE LOS ACTIVOS

Se sugiere que los activos de la SECAB tengan asignados un propietario, responsable para el control adecuado, garantizando mantener la protección adecuada de los activos de la organización.

9.1.1 Inventario de Activos. Se identifican los activos con mayor relevancia de la SECAB, como se aprecia en el cuadro 13:

Cuadro 13. Inventario de activos relevantes

Tipo	Activo
Información	Bases de Datos
	Contratos
	Manuales de Usuario
	Manuales de Configuración
	Documentos de Auditoria
Software	Software Sistemas de Información
	Sistemas Operativos
Hardware	Equipos de Escritorio
	Servidores
	Switch
	Cd's con Informes
Servicios	Energía
	Red
	Agua
Intangible	Reputación
Fuente: La Autora	

Para conocer el inventario detallado (Véase el Anexo B)

9.1.2 Propietario de los Activos. Se recomienda que los activos identificados en el…numeral 9.1.1…, posean un propietario; este término no significa que las personas poseen derechos de propiedad real sobre el activo asignado, solo hace relación de identificación al individuo que posee una responsabilidad aprobada por la SECAB, en donde cumple lo siguiente:

- Garantizar que la información y los activos de procesamiento sean clasificados correctamente.
- Definir y revisar las clasificaciones del acceso asignado.

Es de aclarar que, las labores de rutina se pueden delegar, pero estas siguen siendo responsabilidad del propietario (ver cuadro 14).

Cuadro 14. Propietario de activo

Tipo	Activo	Propietario
Información	Bases de Datos	Responsable de Sistemas
	Contratos	Responsable de Contratación
	Manuales de Usuario	Responsable del área de donde se requiera el uso
	Manuales de Configuración	Responsable de Sistemas
	Documentos de Auditoria	Responsable de Administrativa
Software	Software Sistemas de Información	Responsable de Sistemas
	Sistemas Operativos	Responsable de Sistemas
Hardware	Equipos de Escritorio	Usuario Asignado
	Servidores	Responsable de Sistemas
	Switch	Contratista de Red
	Cd's con Informes	Responsable Administrativa
Servicios	Energía	Contacto por medio de Administrativa
	Agua	
	Red	Contacto por medio de sistemas
Intangible	Reputación	Todas las partes involucradas con la SECAB.
Fuente: La Autora		

9.1.3 Uso Aceptable de los Activos. Es necesario que todas las partes contratadas por la SECAB, sigan, respeten y cumplan las reglas para el uso aceptable de la información y activos asociados con el servicio de procesamiento de la misma.

En dónde; se sugiere que la responsabilidad de los empleados sea la siguiente:

- **Evitar la Divulgación inadecuada de la información**
    - No divulgar información, durante o después del objeto contractual; exceptuando si esta es necesaria para cumplir su objeto laboral dictaminado por la SECAB o en caso de que la ley lo exigiera.
- **Acceso a los sistemas de información**
    - Los accesos son limitados de acuerdo a la labor que se necesita ejercer, por ende no es deber del mismo, buscar, leer o escuchar información alguna a la que este, no esté autorizado; si este llegase a requerir acceso debe obtener la autorización necesaria sobre el activo.
    - Luego de que la parte termine su objeto contractual, realizará la entrega de todos los sistemas, dispositivos y demás mecanismos de información a la persona encargada del área, dejando constancia sobre dicha entrega, indicando también que no retiene información alguna.
- **Prevención al acceso no autorizado**
    - La parte no compartirá y divulgará contraseñas, los equipos portátiles estarán asegurados con métodos de encriptación designados por el oficial de seguridad.
    - Se restringirá el uso de cualquier tipo de herramienta que permita evadir los controles de seguridad, establecer medidas para el bloqueo de los equipos cuando este se encuentre inactivo por más de 5 minutos; Así mismo, es necesario concienciar a los usuarios de cerrar sesión y/o apagar los equipos de cómputo al finalizar su labor, esto podrá ser mediante campañas como fondos o pantallas de bloqueo y demás actividades que se puedan considerar.
    - El cuarto de almacenamiento y de más sitios que contengan información importante contarán con los controles físicos correspondientes que prevengan los accesos a personal no autorizado.

- **Uso Adecuado de los Sistemas**

    - No se utilizaran los activos de la SECAB para ver, recibir o almacenar material inadecuado, ofensivo, ilegal o transmitir comunicaciones abusivas, amenazantes o engañosas.

    - No se cambiará ni alterara de su forma original alguna parte del hardware o software que se le haya entregado y/o asignado por parte de la SECAB, si se requiere alguna modificación o cambio de alguna de las partes, se debe notificar al área de sistemas, quién asignará a la persona correspondiente para realizar dicha acción.

- **Prohibición del uso de medios externos**

    - La parte responsable no almacenará ningún tipo de información perteneciente y/o proveniente de la SECAB, en medios que no sean propiedad de la organización o que no estén contratados.

    - No se podrá utilizar los siguientes medios para establecer un acuerdo formal o procesar información

        - Correos electrónicos personales
        - Redes externas para compartir archivos
        - Redes sociales o foros.

Adicionalmente, se sugiere que es Responsabilidad de Terceros:

- Cuando la SECAB proceda a realizar contratos con terceros y estos tengan acceso a la información, el área de contratación deberá clausular lo siguiente:

    - Cumplimiento de todas las políticas de privacidad.
    - Informar sobre cualquier incidente supuesto o real de seguridad.

- Se debe tener en cuenta los incumplimientos sobre las políticas mencionadas o las que se establezcan con finalidad, para establecer las medidas disciplinarias correspondientes.

9.2 CLASIFICACIÓN DE LA INFORMACIÓN

La información debe ser debidamente protegida de accesos no autorizados, divulgación o destrucción sin importar en donde esta se encuentre almacenada. Para ello es indispensable su clasificación, viendo las necesidades y prioridades de protección en cuanto al manejo de la información. En el cuadro 15 se puede evidenciar la clasificación de información propuesta.

9.2.1 Directrices de Clasificación. Para la clasificación, se estipulan tres tipos: información pública, información Privada, información reservada y confidencial, teniendo en cuenta los requisitos de confidencialidad, integridad y disponibilidad.

Cuadro 15. Clasificación de la información

Requisitos	Clasificación			
	Pública	**Interna**	**Confidencial**	**Reservada**
Confidencialidad	Información que puede ser conocida y utilizada sin autorización	Información que puede ser conocida y utilizada por todo el personal de la organización y los Ministerios de países miembros	Información que solo puede ser conocida y utilizada por un grupo determinado para su trabajo.	Información conocida y utilizada por el personal de mayor cargo en la SECAB y Ministerios
Integridad	Información que al ser modificada puede ser solucionado de manera rápida sin que tenga afectación	Información que al ser modificada sin autorización, podría ocasionar pérdidas leves	Información que al ser modificada sin autorización, puede ser difícil su reparación, ocasionando pérdidas significativas	Información que al ser modificada sin autorización, no podrá ser reparada, ocasionando pérdidas graves
Disponibilidad	Información que al no presentar accesibilidad, no afecta la operatividad de la SECAB	Información que al no presentar accesibilidad durante 5 días, afectara de manera significativa la operatividad de la SECAB	Información que al no presentar accesibilidad durante 2 días, ocasionará afectación significativa en la operatividad.	Información que al no presenta accesibilidad durante 1 día, ocasionará afectación significativa en la operatividad de la SECAB con Ministerios
Fuente: La Autora				

9.2.2 Etiquetado y manejo de la información. De acuerdo a la clasificación de la información definida…en el numeral 9.2.1…se recomienda establecer procedimientos para el etiquetado en formatos físicos y electrónicos.

Si la información no ha sido clasificada, el personal de la SECAB, rotulará la información sobre la cual se tenga conocimiento, no obstante este no podrá asumir que aquella información que no se encuentre catalogada como confidencial es de concernencia pública, la información que no esté catalogada como pública, privada o confidencial se asumirá como reservada.

Cuando se tengan dudas sobre la clasificación de la información en las categorías mencionadas…en el numeral 9.2…., el personal estará en su debido deber y derecho de consultar con la persona de mayor rango dentro de la SECAB.

El intercambio de información con los Ministerios de Educación se realizará por los medios aprobados institucionalmente.

- Correo Institucional.
- Intranet.
- Papel.
- Medio extraíble, manejando contraseñas de apertura.

En el presente documento se da a conocer una guía para rotular adecuadamente la información confidencial de la SECAB. (Ver Anexo C)

10. SEGURIDAD DE LOS RECURSOS HUMANOS

10.1 ANTES DE LA CONTRATACIÓN LABORAL

Se recomienda que esta política se aplique para todo el personal de la SECAB que realice labores dentro de la secretaría, sin importar la relación contractual que se tenga; es responsabilidad de cada persona velar por el cumplimiento de esta política.

10.1.1 Roles y responsabilidades. El líder del área de recursos humanos será responsable de informar a todo el personal que ingresa acerca de las políticas de seguridad de la información, adicionalmente informará al área de sistemas sobre los ingresos, retiros y modificaciones del perfil del personal.

El líder de cada área es responsable de definir el perfil del personal que ingresa a la secretaría y de autorizar los accesos a los recursos de la misma, asimismo es su responsabilidad recibir equipos, software, documentación, manuales e información producida por el personal al momento de su retiro.

El área de seguridad informática es el responsable de promover campañas donde se muestre la importancia de cumplir a cabalidad las directrices de esta política por medio de correos, capacitaciones y salvapantallas con tips de seguridad.

Cada usuario es responsable de reportar fallas o anomalías en el funcionamiento de cualquier sistema, así como de la sospecha de violaciones a la seguridad de la secretaría, ya sea por virus informático o por acceso no autorizado a equipos e instalaciones de la secretaría.

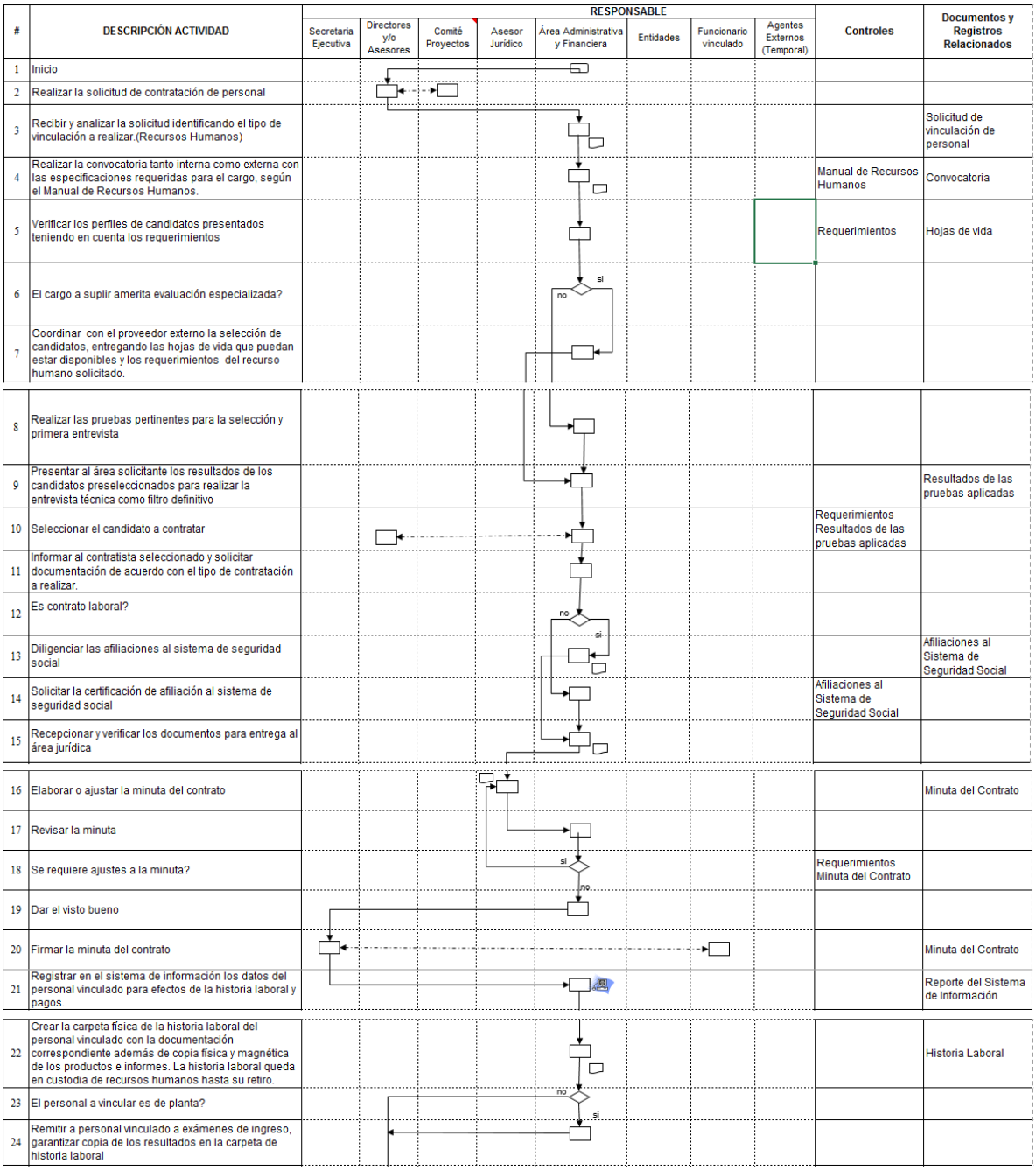
Evitar utilizar los recursos de sistemas de forma que pueda atentar con la seguridad de la información, por ejemplo:

- Envío de cadenas de correo
- Envío de usuarios, IP y contraseñas por correo o chat
- Actividades no relacionadas con la operación de la SECAB

10.1.2 Selección

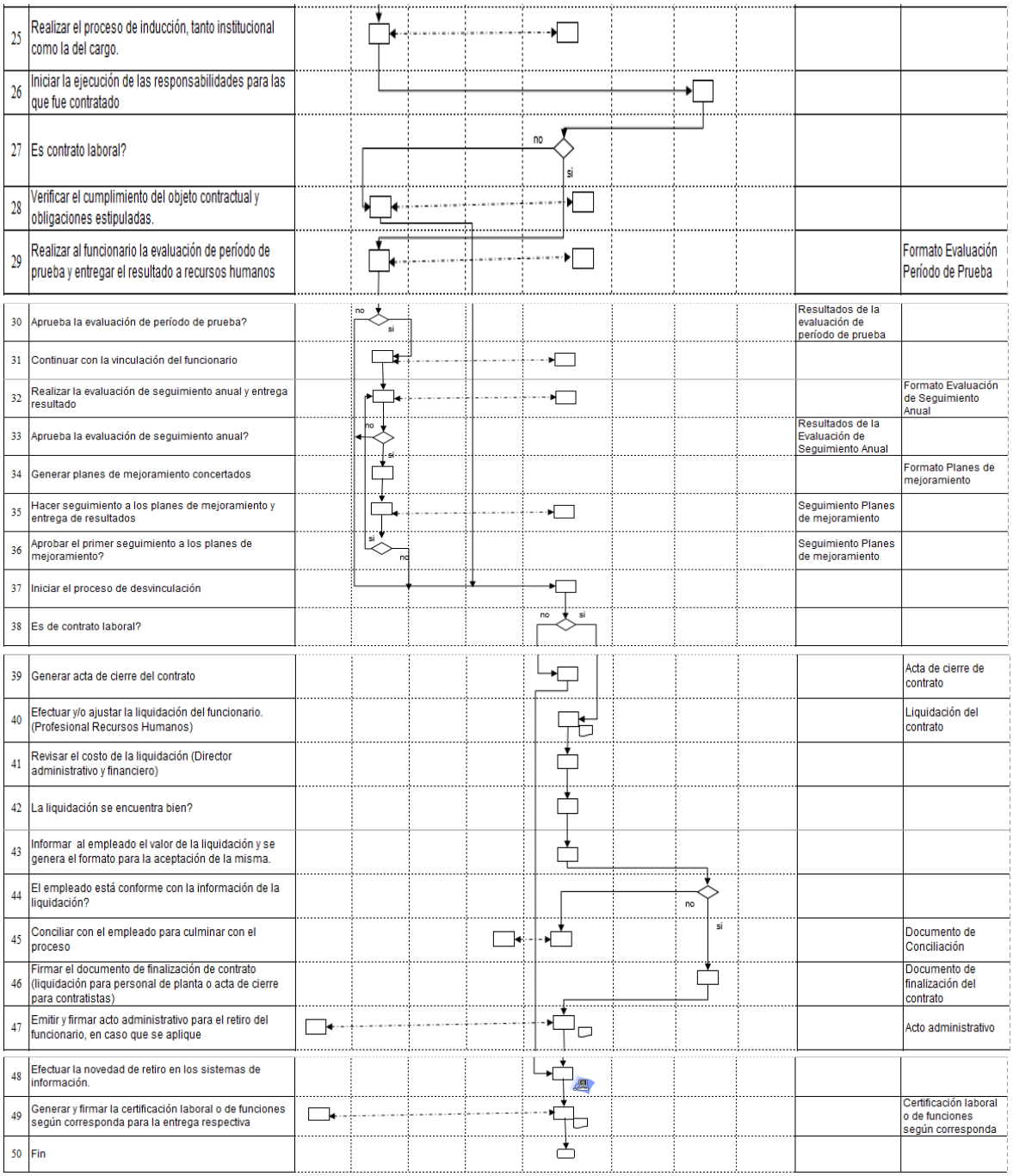
Para el proceso de selección se tiene en cuenta el diagrama que aparece en la figura 1.

Figura 1. Proceso de selección



#	DESCRIPCIÓN ACTIVIDAD	RESPONSABLE								Controles	Documentos y Registros Relacionados
		Secretaria Ejecutiva	Directores y/o Asesores	Comité Proyectos	Asesor Jurídico	Área Administrativa y Financiera	Entidades	Funcionario vinculado	Agentes Externos (Temporal)		
1	Inicio										
2	Realizar la solicitud de contratación de personal										
3	Recibir y analizar la solicitud identificando el tipo de vinculación a realizar.(Recursos Humanos)										Solicitud de vinculación de personal
4	Realizar la convocatoria tanto interna como externa con las especificaciones requeridas para el cargo, según el Manual de Recursos Humanos.									Manual de Recursos Humanos	Convocatoria
5	Verificar los perfiles de candidatos presentados teniendo en cuenta los requerimientos									Requerimientos	Hojas de vida
6	El cargo a suplir amerita evaluación especializada?										
7	Coordinar con el proveedor externo la selección de candidatos, entregando las hojas de vida que puedan estar disponibles y los requerimientos del recurso humano solicitado.										
8	Realizar las pruebas pertinentes para la selección y primera entrevista										
9	Presentar al área solicitante los resultados de los candidatos preseleccionados para realizar la entrevista técnica como filtro definitivo										Resultados de las pruebas aplicadas
10	Seleccionar el candidato a contratar									Requerimientos Resultados de las pruebas aplicadas	
11	Informar al contratista seleccionado y solicitar documentación de acuerdo con el tipo de contratación a realizar.										
12	Es contrato laboral?										
13	Diligenciar las afiliaciones al sistema de seguridad social										Afiliaciones al Sistema de Seguridad Social
14	Solicitar la certificación de afiliación al sistema de seguridad social									Afiliaciones al Sistema de Seguridad Social	
15	Recepcionar y verificar los documentos para entrega al área jurídica										
16	Elaborar o ajustar la minuta del contrato										Minuta del Contrato
17	Revisar la minuta										
18	Se requiere ajustes a la minuta?									Requerimientos Minuta del Contrato	
19	Dar el visto bueno										
20	Firmar la minuta del contrato										Minuta del Contrato
21	Registrar en el sistema de información los datos del personal vinculado para efectos de la historia laboral y pagos.										Reporte del Sistema de Información
22	Crear la carpeta física de la historia laboral del personal vinculado con la documentación correspondiente además de copia física y magnética de los productos e informes. La historia laboral queda en custodia de recursos humanos hasta su retiro.										Historia Laboral
23	El personal a vincular es de planta?										
24	Remitir a personal vinculado a exámenes de ingreso, garantizar copia de los resultados en la carpeta de historia laboral										

Figura 1. (Continuación)



Fuente: Tomado del Registro Digitalizado de diagrama procedimientos RRHH SECAB

Durante el procesos determinado por el área de Recursos Humanos, se tienen en cuenta toda la documentación requerida para su debida validación, entre ello antecedentes, reportes disciplinarios, confirmación de títulos y experiencias, referencias, validación del documento de identificación, entre otros, requeridos con la documentación en su hoja de vida.

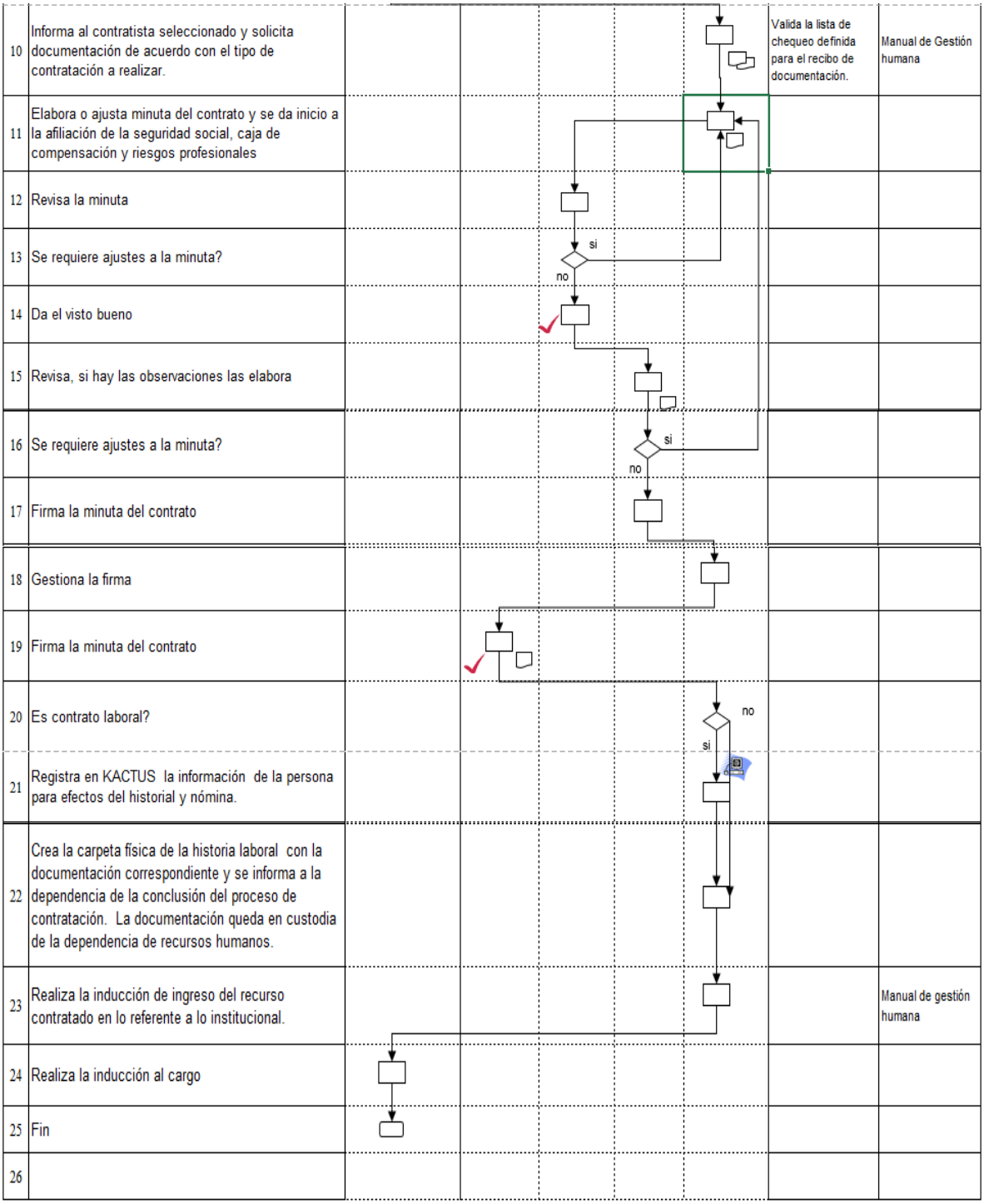
10.2 INGRESO

Para el ingreso las consideraciones a valorar se relacionan en la figura 2.

Figura 2. Proceso de ingreso

#	DESCRIPCIÓN ACTIVIDAD	RESPONSABLE					Controles	Documentos y Registros Relacionados
		Direcciones de Programa	Secretaria Ejecutiva	Asesor Jurídico	Contratista Aspirante	Área Administrativa y Financiera Financiera		
1	INICIO							
2	Elabora solicitud de contratación de recurso humano. De acuerdo con lo establecido en el manual de gestión humana.							Manual de Gestión humana. Formato solicitud de contratación
3	Estudio y aprobación de necesidades de contratación .						Visto bueno	
4	Se aprueba la solicitud?							
5	Requiere selección del recurso humano?							
6	Realiza la selección del recurso humano de acuerdo con las características y perfiles requeridos. (Proceso: 3.1.2.1 Selección de Recurso Humano)							
7	Recibe las hojas de vida del candidato o candidatos, programa y realiza la entrevista o las entrevistas necesarias para escoger al recurso adecuado conforme a las necesidades. Escoge al candidato y lo presenta a la secretaria ejecutiva.							
8	El candidato es aprobado?							
9	Informa a recursos humanos acerca del candidato escogido							

Figura 2. (Continuación)



10	Informa al contratista seleccionado y solicita documentación de acuerdo con el tipo de contratación a realizar.	Valida la lista de chequeo definida para el recibo de documentación.	Manual de Gestión humana
11	Elabora o ajusta minuta del contrato y se da inicio a la afiliación de la seguridad social, caja de compensación y riesgos profesionales		
12	Revisa la minuta		
13	Se requiere ajustes a la minuta?		
14	Da el visto bueno		
15	Revisa, si hay las observaciones las elabora		
16	Se requiere ajustes a la minuta?		
17	Firma la minuta del contrato		
18	Gestiona la firma		
19	Firma la minuta del contrato		
20	Es contrato laboral?		
21	Registra en KACTUS la información de la persona para efectos del historial y nómina.		
22	Crea la carpeta física de la historia laboral con la documentación correspondiente y se informa a la dependencia de la conclusión del proceso de contratación. La documentación queda en custodia de la dependencia de recursos humanos.		
23	Realiza la inducción de ingreso del recurso contratado en lo referente a lo institucional.		Manual de gestión humana
24	Realiza la inducción al cargo		
25	Fin		
26			

Fuente: Tomado del Registro Digitalizado de diagrama procedimientos RRHH SECAB

Mediante el proceso de contratación y firma de contrato, se podrán ver reflejados los términos y condiciones laborales estipulados por la SECAB, en donde la parte aceptará con la firma, los procedimientos internos referentes a la seguridad; entre otros, acuerdos de confidencialidad, políticas de seguridad establecidas, uso adecuado de activos y manejo de información los cuales se encuentran definidas institucionalmente.

El compromiso de la Secretaria Ejecutiva es exigir a la parte contratada y terceras partes el cumplimiento de las políticas y procedimientos establecidos dentro de la SECAB.

10.3 RETIRO

El proceso de retiro se observa en la figura 3.

Figura 3. Proceso de retiro

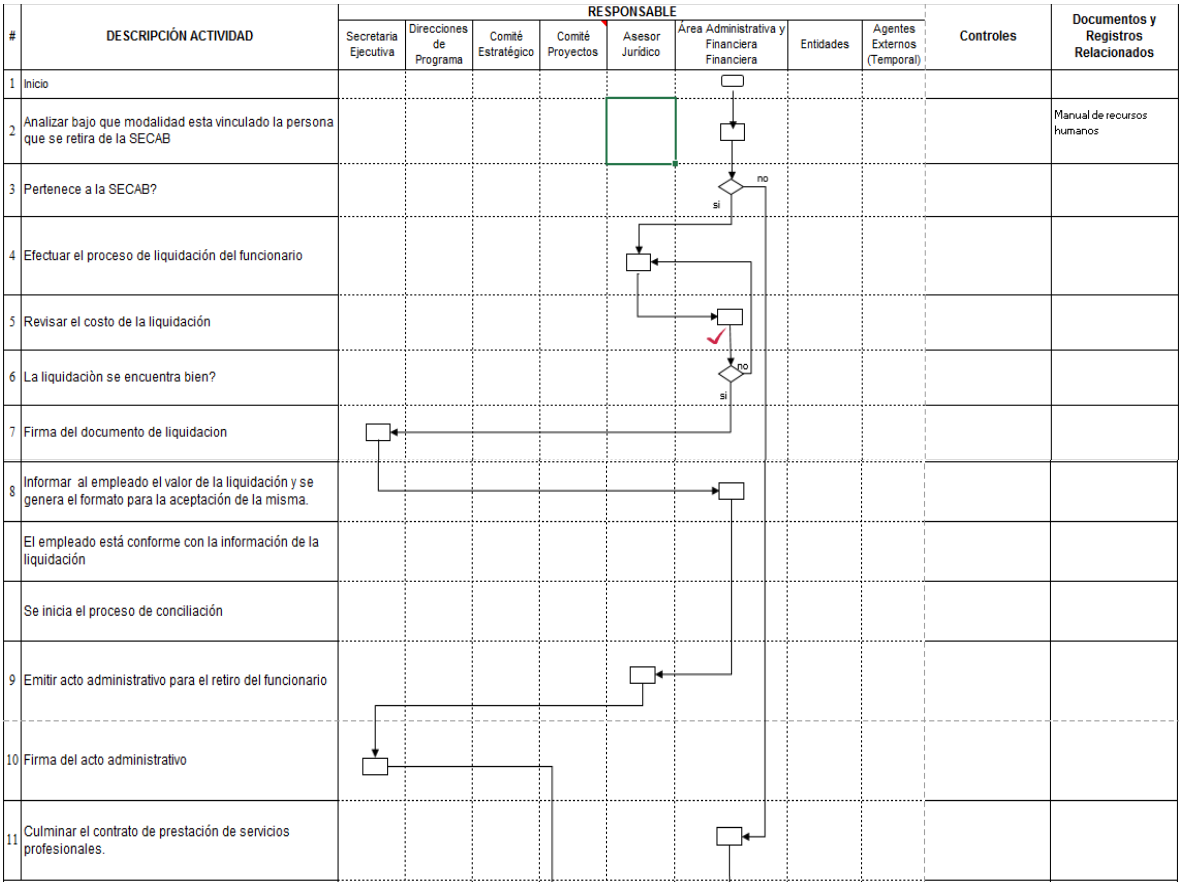
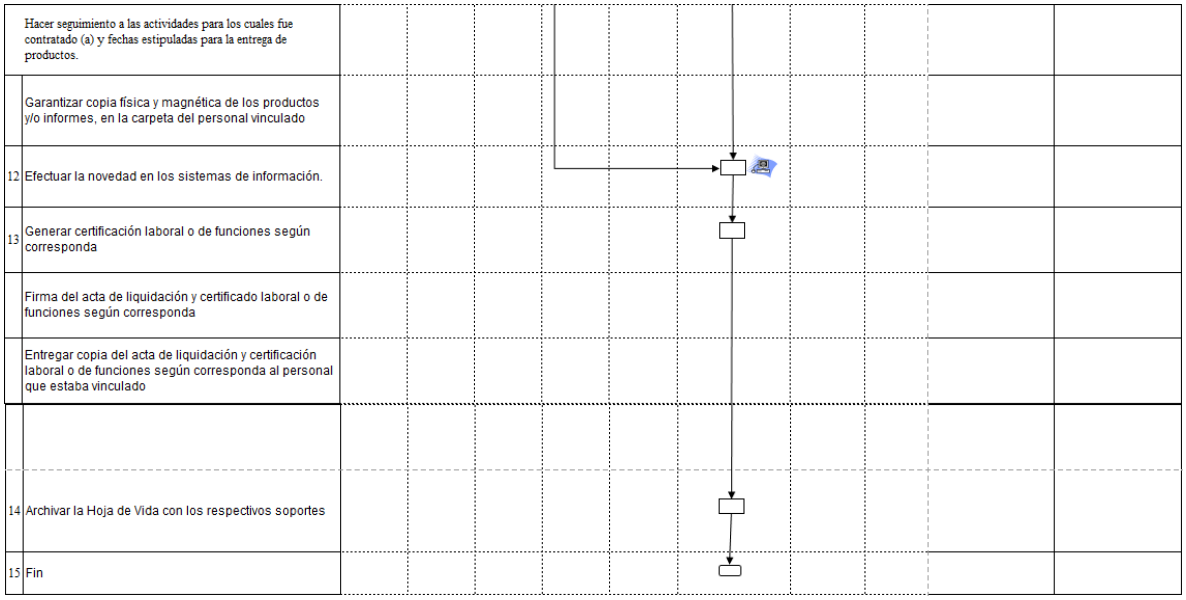


Figura 3. (Continuación)



Fuente: Tomado del Registro Digitalizado de diagrama procedimientos RRHH SECAB

El cambio de responsabilidades, objeto contractual y terminación de contrato, no dará lugar al no cumplimiento permanente de los acuerdos y cláusulas de confidencialidad.

El área de Recursos Humanos debe realizar la coordinación con el jefe de área sobre las responsabilidades nuevas que se asignen, sobre la parte que ingrese o cambie de responsabilidad.

La parte que realice cambio de responsabilidades no tendrá que ser capacitado nuevamente en temas de seguridad, se supondrá que este aún tiene claro los procedimientos de normas y políticas definidas; esto solo cambiará, si para ese tiempo se han realizado modificaciones significativas en la SECAB.

10.3.1 Devolución de Activos. Se propone que al finalizar o dar por terminado el objeto contractual, la parte, deberá hacer devolución de todos los activos que hayan sido asignados pertenecientes a la SECAB; esto se hará mediante la formalización en un acta.

Se propone que el proceso de devolución incluya:

- Token
- Tarjeta de Acceso principal
- Documentos Físico y digitales
- Equipo de Escritorio
- Equipo portátil
- Carnet de identificación institucional
- Manuales
- Dispositivos de almacenamiento externo
- Impresora
- Material de papelería

Si a la parte no le fue asignado ningún activo físico de la SECAB, este quedara expresamente documentado.

El Área Legal, Área Administrativa y el Área de Recursos Humanos, deberán incorporar los términos que sean requeridos en los respectivos contratos para el cumplimiento del control en la devolución de activos.

10.3.2 Retiro de los derechos de acceso. Al finalizar o dar por terminado el objeto contractual, es necesario que sean removidos todos los accesos y derechos de uso, si la parte ha sido asignada a labores o responsabilidades diferentes, estos cambios deberán realizarse de acuerdo a sus nuevas funciones.

El área de Recursos Humanos notificará el retiro o cambio de labores al área de sistemas a su vez que al oficial de seguridad, con el fin de que estos identifiquen los acceso de sistemas, información, carpetas a los que la parte tuviese derecho de acceder, considerando la posibilidad de modificar o quitar los derechos de accesos; así mismo, cuando la parte tuviese conocimiento de contraseñas a sistemas de acceso permanente, se tomarán en cuenta para realizar los cambios pertinentes.

Se sugiere que si la parte fue retirada o se ha finalizado su objeto contractual:

- Sea eliminado su usuario de acceso en identificación del dominio.
- Sea eliminado su usuario de acceso a los sistemas de información.
- Sea eliminado su usuario de las listas en donde se comparten documentos.
- Si la parte era propietario de carpetas o documentos que se compartían, se asigne a un responsable para dicho control.

11. SEGURIDAD FÍSICA Y DEL ENTORNO

La seguridad física y del entorno es uno de los factores más importantes para lograr un mayor control y prevención de daño, pérdida o robo de los activos en la organización.

11.1 ÁREAS SEGURAS

Se sugiere evitar el acceso no autorizado sobre los servicios de procesamiento de información sensible, evitando así posibles daños o interferencias sobre estos servicios de la SECAB.

11.1.1 Perímetro de seguridad física. La SECAB necesita utilizar perímetros de seguridad física para dar protección, a las áreas en donde se almacenan los servicios de procesamiento de la información sensible o cualquier área que sea considerada crítica para el adecuado funcionamiento de los sistemas.

Para la estrategia de diseño e implementación del perímetro de seguridad, se requiere definir por el área de sistemas y el oficial de seguridad, según lo analizado en la evaluación de riesgos.

En donde se aconseja tener en cuenta las siguientes pautas para establecer los perímetros de seguridad física:

- Que activos se requieren proteger
- Identificación del área que se requiere proteger, de acuerdo a los activos considerados dentro del perímetro.
- Qué tipo de protección física requiere el área.

11.1.2 Controles de acceso físico. Las áreas catalogadas como críticas o que almacenen servicios de procesamiento con información sensible, necesitan estar protegidas con controles de acceso adecuados que aseguren que solo accede la persona autorizada.

Si una parte no autorizada, necesita tener acceso, este deberá mediar los propósitos específicos para ser autorizado, generando un registro sobre el tiempo en el cual ha ingresado, tiempo de salida, función a realizar y quien dio autorización a su ingreso.

En donde, se propone que:

- Los accesos al área de servidores y cableado, sean aprobados por el área de sistemas, y estos a su vez, supervisados por un ingeniero durante las funciones a desempeñar dentro del área.
- Se debe tener una bitácora de ingresos, en lugar visible para su debido diligenciamiento del personal externo o ajeno a la SECAB.
- Los permisos de acceso al Edificio, se deben modificar al momento de un cambio o desvinculación.

11.1.3 Protección contra amenazas externas y ambientales. Es importante, tomar medidas pertinentes, para evitar daños ocasionados por las amenazas naturales y externas ocasionadas por el hombre.

En ese sentido se propone tener en cuenta los siguientes parámetros para evitar daños perjudiciales para la SECAB.

- Los materiales catalogados como peligrosos o combustibles, deben estar almacenados a una distancia prudencial de las áreas protegidas.
- Los insumos de papelería no deben ser almacenados a gran cantidad.
- Disponer de extintores y demás herramientas apropiadas para disipar el fuego, deben estar en lugares estratégicamente visibles.
- Las áreas que deben ser protegidas, deben contar monitoreo de cámaras y sistema de alarma.
- Los servidores deben contar con un control sobre los niveles de temperatura y humedad.
- No permitir el consumo de alimentos y bebidas dentro de las áreas que cuenten con servicio de procesamiento de información.
- El área de sistemas debe proveer y mantener las condiciones ambientales, garantizando así la operación continua de los equipos en el área de servidores y fuera de ella.

11.2 SEGURIDAD DE LOS EQUIPOS

En este punto es necesario evitar el daño, robo o disposición de los activos ante el peligro, provocando interrupción de la operación en la SECAB.

Por tal razón, se aconseja prever la protección del equipo dentro de la SECAB, y también fuera de la organización, evitando que personas no autorizadas tengan acceso a la información en caso de robo.

11.2.1 Ubicación y protección de los equipos. El entorno de los equipos es uno de los factores fundamentales a la hora de brindar seguridad a los equipos, ya que con ello se pueden reducir los peligros, falla ambiental y accesos no autorizados. En ese sentido, se recomiendan las siguientes medidas:

- El área de sistemas, establecerá un estándar de configuración adecuada para todo los equipos que pertenezcan a la SECAB.
- Los equipos tecnológicos, estarán aislados de cualquier ubicación que pueda afectar el funcionamiento de los mismos.
- El área de sistemas y el oficial de seguridad, propondrá alineamientos para la protección de la información, cuando los equipos ya no sean operativos o se realicen cambios de ellos.
- El área de sistemas es el único encargado de realizar movimientos de los equipos o cambios de partes.
- Las partes que tengan asignados equipos propiedad de la SECAB, bloquearán sus estaciones de trabajo en el momento que se retiren del sitio.
- No se dejará encendido el equipo, en horas no laborales.
- En caso de que el equipo propiedad de la SECAB, sea extraviado o causal de robo, se debe informar de manera inmediata al área administrativa para que se realice el proceso correspondiente.

11.2.2 Servicios de suministro. Los equipos necesitan estar protegidos por posibles fallas de energía y otras causales por fallas en los servicio de suministro.

Para ello se sugiere:

- Disponer de toma corriente y líneas de suministros de energía que estén reguladas.
- Que la SECAB cuente con protección contra descargas de energía en el edificio donde se encuentran ubicadas sus instalaciones.
- Poseer un sistema interrumpible de energía como UPS o planta eléctrica, asegurando el apagado regulado de los equipos de cómputo.
- Interruptores de suspensión en la energía cuando se presenten emergencias.
- Continuidad en el servicio de agua para asegurar la alimentación del aire acondicionado que se encuentra en el cuarto de servidores y el sistema contra incendios de la SECAB.

11.2.3 Seguridad del cableado. El cableado de energía y telecomunicaciones utilizados en la SECAB. Necesita contar con protección contra daños e intercepción.

Para ello se propone lo siguiente:

- Dar cumplimiento con los requisitos técnicos vigentes de la Republica de Colombia.
- Garantizar que el cableado de energía esté debidamente separado del cableado de red, evitando así posibles interferencias.
- El cableado contará con canaletas para su adecuada protección.
- Utilizar diferenciaciones entre el cableado, evitando conexiones erróneas.
- Contar con un plano de cableado, identificando fácilmente los puntos ante posibles fallas.
- El área de sistemas es el único encargado de realizar cambios o movimientos de cables.

11.2.4 Mantenimiento de los equipos. Los equipos de cómputo requieren contar con el debido mantenimiento para asegurar su disponibilidad.

Para ello se sugiere lo siguiente:

- Contar con un cronograma anual de mantenimientos para los equipos de la SECAB.
- Dar cumplimiento al cronograma de mantenimiento, que se encuentra definido.
- Realizar mantenimientos y pruebas funcionales después de realizado, a las UPS o plantas eléctricas, aire acondicionado, servidores, equipos de escritorio, portátiles, impresoras, equipos de comunicaciones y demás equipos que conformen la estructura tecnológica de la SECAB.
- Registrar fallas durante los mantenimientos, registrando la falla presentada, la fecha y persona que realizo el mantenimiento.
- Los mantenimientos serán realizados por personas que tengan el conocimiento adecuado y la expertica sobre los equipos tecnológicos a los cuales sean efectuados los mantenimientos.

11.2.5 Seguridad de los equipos fuera de las instalaciones. Si se requiere trabajar fuera de la SECAB, con un equipo asignado de la propiedad de la organización, es necesario tener en cuenta los diversos riesgos a los cuales se encuentra expuesto.

Con el fin de dar una protección se propone hacer lo siguiente:

- Tener autorización expresa por un personal superior para sacar el equipo de la SECAB.
- Diligenciar un formato, que indique la fecha, hora, serial y marca del dispositivo tecnológico que se va a sacar, el cual será almacenado y registrado en la bitácora de la recepción.
- Reportar cuando el equipo se encuentre nuevamente dentro de las instalaciones de la SECAB.
- La persona que retira el equipo será expresamente responsable por el elemento y la información que en él se contenga.
- El área de sistemas y el oficial de seguridad, deben plantear mecanismos y estrategias que permitan proteger la confidencialidad del activo tecnológico, fuera de la SECAB.
- Los equipos no deben ser expuestos en zonas con alta carga de electromagnetismo

12. GESTIÓN DE COMUNICACIONES Y OPERACIONES

Lo que se busca es garantizar y establecer definidamente responsabilidades y procedimientos que permitan el funcionamiento adecuado de la operatividad en las comunicaciones.

12.1 PROCEDIMIENTOS OPERACIONALES Y RESPONSABILIDADES

Se establecen todas las responsabilidades y procedimientos para la gestión y operación de los servicios de procesamiento de información.

12.1.1 Documentación de los procedimientos de operación. Se sugiere garantizar la documentación de los procedimientos relacionados con la operación de los elementos tecnológicos que apoyan la continuidad de la SECAB.

A continuación se relacionan algunos procesos documentados (Véase detalle en Anexo D):

- Inicio, reinicio y apagado de los equipos de cómputo.
- Copias de respaldo
- Mantenimiento de equipos
- Gestión del correo.
- Creación de usuarios en el directorio activo.
- Asignación de equipos.
- Solicitud de acceso a carpetas compartidas.

Este tipo de documentos se recomienda sean tratados como formales, debidamente clasificados y que sus cambios sean aprobados por el oficial de seguridad.

12.1.2 Gestión del cambio. Todos los cambios que se necesiten realizar, en el software, procedimientos o hardware, se notificarán al área responsable para su debida gestión.

- **Control cambio de hardware:**

Si se requiere cambiar una parte del hardware por daño, se puede notificar al área de sistemas, quién realizará la gestión del cambio necesario, notificando al área de administrativa para control del inventario.

- **Control cambio de software:**

Si se requiere cambiar el sistema operativo de alguno de los activos, se sugiere al área de sistemas y al oficial de seguridad, ver la viabilidad del cambio de software, anteponiendo las generalidades de seguridad, mantenimiento, costos y si este es viable.

Adicionalmente, cuando se requiera la instalación de un software para el cumplimiento de las labores, este será aprobado por el jefe de área, quien deberá enviar la solicitud de instalación al área de sistemas con la justificación necesaria para la instalación.

Se mantendrá actualizado y monitoreado el software de la SECAB, para la detección y control de códigos maliciosos.

En todos los casos el oficial de seguridad, deberá velar porque dichos controles no afecten la seguridad de la SECAB.

Antes de realizar cualquier cambio radical se propone tener en cuenta:

- El impacto que se generara, en el desempeño actual.
- Recuperación ante errores o fallas que se puedan generar.
- Asegurar que la nueva instalación no afectara de forma significativa el funcionamiento de los sistemas existentes.
- Si se pone en vigencia un nuevo sistema, realizar capacitaciones para el uso del nuevo componente.

12.2 GESTIÓN DE LA PRESTACIÓN DEL SERVICIO POR TERCERAS PARTES

La SECAB es la encargada de mantener los niveles de seguridad con la parte prestadora del servicio (terceros), según lo acordado y establecidos con estos. Así también, de la gestión de los cambios, asegurando que los servicios prestados cumplen con los requisitos acordados con los terceros y de los acuerdos sobre disposiciones de seguridad, enfocados en controles que sean implementados, mantenidos y operados por la tercer parte.

En ese sentido se sugiere que:

- Los supervisores asignados para los contratos con terceros y el oficial de seguridad, administren los cambios ejercidos por los proveedores, manteniendo y garantizando los niveles de seguridad establecidos con los terceros.
- Establecer mecanismo de monitoreo funcionales para la detección de nuevos riesgos.
- Verificar las conexiones seguras, cifrados y métodos de transmisión desde la SECAB, hacia el tercero.
- Verificación en el cumplimiento de los acuerdos de seguridad.

12.3 PLANIFICACIÓN Y ACEPTACIÓN DEL SISTEMA

El responsable que sea designado para liderar un proyecto de nuevo sistema, es el encargado de realizar un planteamiento inicial sobre los requisitos técnicos que este requiere, identificando la capacidad de momento que se necesita para dar inicio con la ejecución y una proyección sobre lo que se puede requerir de acuerdo con nuevas funciones dentro de la SECAB.

Luego de ello, el responsable, toma criterios de aprobación para el nuevo sistema, se sugiere que estos criterios garanticen que:

- Con el nuevo sistema no se verá afectado el rendimiento de los equipos.
- El nuevo sistema no afectará de manera negativa a los sistemas existentes.
- Las actualizaciones no requerirán un cambio en los equipos de trabajo.
- Su uso, no sea complejo para el usuario.

12.4 PROTECCIÓN CONTRA CÓDIGOS MALICIOSOS

Se propone que la SECAB proporcione los mecanismos que sean necesarios para garantizar la protección de la información y la infraestructura tecnológica que la procesa y almacena, esto con el fin de que el área de sistemas y el oficial de seguridad, adopten los controles necesarios que eviten la modificación en la integridad o algún otro daño ocasionado por un código malicioso.

El oficial de seguridad conjunto al área de sistemas, realizará campañas de concienciación para generar cultura y educación entre las partes.

12.5 RESPALDO DE LA INFORMACIÓN

Es necesario que la SECAB proporcione los medios de almacenamientos externos para las copias de respaldo que se realicen a la información de la organización. De esta forma, los dueños de la información conjunto al área de sistemas definirán la estrategia más adecuada para la generación de dichas copias.

Por tal razón se propone que el almacenamiento de los medios donde se generen las copias, sea realizado en un área con controles de seguridad física y ambiental adecuados. Para estos efectos se propone que:

- El área de sistemas genere estrategias y adopte diferentes procedimientos para la generación, almacenamiento y restauración de las copias de la información, asegurando su integridad y disponibilidad.
- Se disponga de los recursos necesarios que permitan identificar los medios en donde se encuentren las copias respaldo.
- Se cuente con la información debidamente organizada que permita saber la ubicación física, asegurando un acceso rápido de los medios que contienen las copias de respaldo.
- El área de sistemas lleve a cabo pruebas de recuperación sobre los respaldos, asegurando su integridad y disponibilidad.
- Se cuente con un control de custodia sobre los medios.
- Identificar la información más sensible de los usuarios, la cual será respaldada y almacenada debidamente.

12.6 GESTIÓN DE LA SEGURIDAD DE LAS REDES

Es un requisito primordial, asegurar la protección de la información que viaja a través de las redes, manteniendo y controlando adecuadamente el flujo de datos, protegiendo sobre las amenazas que se encuentran en la red, incluyendo características de seguridad.

12.6.1 Controles y seguridad de las redes

En este punto se sugiere lo siguiente:

- Implementar controles, con mecanismos adecuados que permitan el monitoreo del flujo de datos, transportados por la red.
- Establecer estándares técnicos de configuración para los dispositivos que accedan a la red de la SECAB.
- Establecer niveles de seguridad de red e incluirlos con los servicios externos.
- Habilitar solo los protocolos y puertos que sean requeridos, los cuales deben estar debidamente justificados.
- Asegurar la disponibilidad de los recursos que se encuentren en red.
- Monitorear las herramientas de seguridad perimetral implementadas, para detección de intrusos.

12.7 MANEJO DE LOS MEDIOS

Este punto comprende la administración y el uso seguro de los diversos medios donde se encuentra almacenada la información, tales como:

- Memorias USB.
- Discos extraíbles.
- CD y DVD
- Memorias SD y Micro SD

Evitando así la divulgación o retiro de información de manera no autorizada.

12.7.1 Gestión de los medios removibles. Para el uso adecuado de los medios removibles, se sugiere tener en cuenta los siguientes puntos:

- Los medios que contengan información sensible, serán almacenados en un área segura, según esta sea clasificada.
- Los medios que sean reutilizados fuera de la SECAB, contarán con un borrado seguro, antes de salir de la organización, esto con el fin de evitar recuperaciones de la información.
- Si se realiza cambio de medio de almacenamiento de la información, se respaldará en otro medio, para evitar la pérdida de la información.

- Cuando se haya asignado un medio removible, es responsabilidad de quien recibe el medio, su aseguramiento, evitando daños, perdidas, accesos no autorizados o robos.
- Solo se podrá guardar la información en el medio removible que haya sido asignado.
- En caso de robo, pérdida o daño del medio, se notificará al área de sistemas y al oficial de seguridad.

12.7.2 Eliminación de los medios. Es importante tener en cuenta que cuando ya no se requieran los medios removibles, estos pueden ser eliminados de manera segura, utilizando los siguientes procedimientos:

- Los medios que contengan información confidencial, serán eliminados mediante el borrado seguro de datos.
- Si el medio se ha dañado lógicamente, se destruirán físicamente.

12.8 INTERCAMBIO DE LA INFORMACIÓN

Es necesario asegurar la información al momento de ser transferida o intercambiada con otras entidades y/o áreas, sea esta por medio físico o digital, estableciendo controles necesarios para el intercambio de la misma.

12.8.1 Políticas y procedimientos para el intercambio de información

En este aspecto se propone que:

- El área de sistemas brinde las herramientas y métodos necesarios para que la transmisión de la información por medio de la red, sea confiable
- Los intercambios de información de la SECAB con terceros, solo podrán ser efectuados cuando se hayan establecido los acuerdos de intercambio correspondientes.
- El propietario de la información velará, por la no divulgación de parte de terceros a quienes se les haya entregado información; verificando cumplimientos de cláusulas de confidencialidad o acuerdos de intercambio.

- El área de sistemas, definirá procedimientos de intercambio de información por medio de la red.
- El responsable al momento de enviar información por correo electrónico, se asegurará que la dirección de correo es la correcta.
- El propietario de la información, debe asegurarse que la información a intercambiar, sea la estrictamente necesaria.
- La información física enviada a terceros, deberá ser entregada por el personal dispuesto de la SECAB, con un debido seguimiento.
- No se permite el intercambio de información confidencial o reservada, de manera verbal por medio telefónico.

13. CONTROL DEL ACCESO

13.1 POLÍTICA DE CONTROL DE ACCESO

Al momento de definir las políticas es recomendable tener en cuenta las siguientes consideraciones:

- Requerimientos de manera individual y/o a nivel de grupos para el uso y acceso de cada una de las aplicaciones.
- Definición de roles y privilegios de acceso para los usuarios de acuerdo a la necesidad laboral.
- Planeación periódica para la revisión de los controles de accesos.
- Todo lo definido dentro de esta política, deberá ir alineado con las necesidades institucionales de la SECAB.

13.2 GESTIÓN DEL ACCESO DE USUARIOS

Es necesario garantizar que solo puedan acceder los usuarios autorizados, manteniendo procedimientos que permitan controlar dichos accesos a los sistemas, información y demás servicios institucionales que se encuentren a disposición de los funcionarios y contratistas.

13.2.1 Registro de usuarios. Se aconseja tener un registro de la creación, suspensión o desactivación de usuarios para funcionarios y contratistas, los cuales deben estar previamente autorizados, sea por solicitud explicita del jefe del área o Talento humano. Para tal fin se pueden tener en cuenta los siguientes procedimientos:

- Todos los accesos lógicos, serán autenticados con un ID único y contraseña, que permita identificar plenamente el registro de la persona que ingreso.
- Cuando se realicen modificaciones de contratos o retiros de contratistas o funcionarios, se deberán aplicar los cambios de privilegios o desactivaciones de cuentas respectivas, según sea lo requerido.
- Realizar verificaciones periódicas, evitando redundancia en las cuentas de usuarios.

13.2.2 Gestión de privilegios. Al momento de asignar privilegios a la cuenta de usuario se propone tener en cuenta lo siguiente:

- Identificar qué tipo de permisos requiere cada usuario.
- La existencia de un registro del proceso de autorización y privilegios asignados.

13.2.3 Gestión de contraseñas para usuarios. Es recomendable que las contraseñas de acceso cumplan con un mínimo de 8 caracteres, las cuales deben ser alfanuméricas, letras mayúsculas y minúsculas y algún carácter especial.

Se sugiere que todos los contratistas y funcionarios que cuenten con un usuario de acceso, cambien la contraseña con una prioridad mensual.

Adicionalmente, las contraseñas serán bloqueadas por políticas, luego de 3 intentos fallidos de autenticación.

13.3 RESPONSABILIDADES DE LOS USUARIOS

13.3.1 Uso de contraseñas. Es necesario exigir a los usuarios el cumplimiento de buenas prácticas en el uso de las contraseñas, en cuestión de las siguientes pautas:

- Los datos de acceso como ID y contraseña, mantenerlos en secreto.
- Las contraseñas que sean fáciles de recordar y difíciles de adivinar.
- Al momento de asignar la contraseña, que esta no esté relaciona o sugerida por otra persona que la identifique fácilmente.
- No transmitir las contraseñas por medios físicos como papel o de manera virtual.

13.3.2 Equipo de usuario desatendido. Para garantizar la protección adecuada, se recomienda que todos los funcionarios y contratistas:

- Realicen el bloqueo de los equipos de cómputo, antes de retirarse del sitio de trabajo.
- Mantengan políticas de bloqueo automático de la sesión si se detecta inactividad mayor a 5 minutos.
- Apagar los equipos de cómputo al terminar la jornada laboral.

13.4 CONTROL DE ACCESO A LA RED

Se sugiere garantizar el bloqueo al acceso de páginas de contenidos pornográficos, hacking, descargas (FTP) o cualquier otra página que represente riesgo para el organismo mediante el uso de la red, si se requieren excepciones de accesos estas pueden ser aprobadas y notificadas por medio escrito, del jefe inmediato o según sea su jerarquía mayor, debidamente justificadas en los procesos laborales que se ejercen. Todo esto será sujeto de aprobación por parte del oficial de seguridad.

13.4.1 Autenticación de usuarios para conexiones externas. Este tipo de autenticaciones pueden ser notificadas por el jefe de área, con su respectiva descripción del porque se necesita la conexión de acceso remoto y el tiempo de esta, luego el oficial de seguridad puede aprobar dicho acceso y la herramienta utilizada para este tipo de conexión.

13.5 CONTROL DE ACCESO AL SISTEMA OPERATIVO

Se recomienda el uso de medios o herramientas de seguridad que permitan restringir el acceso a usuarios no autorizados, llevando un control y monitoreo sobre lo siguiente:

- Mantener registros por medio de la activación de logs para visualizar intentos fallidos o exitosos de autenticación en los sistemas.
- Obligar el uso de ID y contraseñas para los accesos, determinando así responsabilidades.
- Definir por medio de políticas que los funcionarios y contratistas puedan realizar el cambio de sus propias contraseñas.

- No permitir que las contraseñas puedan ser visualizadas en texto claro, cuando son digitadas.
- Forzar mediante el Directorio Activo a que el usuario cambie su contraseña, cuando esta es asignada provisionalmente por el administrador del sistema.
- Establecer mediante política institucional la activación de protectores de pantallas, con el fin de evitar que otras personas puedan observar su información, tras una inactividad momentánea.

14. CONCLUSIONES

Tras realizar la propuesta anterior se concluye lo siguiente:

- Después de elaborar el diagnóstico actual de la SECAB se detectan diversos riesgos a los que se está enfrentando el organismo sin saber el tipo de afectación que este pueda representar, esto pese al desconocimiento ya que desde las dos últimas administraciones no se había realizado un levantamiento de información que les permitiera visualizar los riesgos a los cuales se enfrentan sus activos tecnológicos y las consecuencias tras el impacto que se dé.

- La información por ser el activo más importante, requiere de planes eficientes que permitan minimizar los riesgos ante las diversas vulnerabilidades, luego del análisis realizado, se determina que la SECAB no cuenta con los controles necesarios dentro del organismo y pese a las diversas administraciones en el área de sistemas, nunca se han presentado planes de mejora o en algún otro caso los riesgos a los que se encuentran expuestos por las vulnerabilidades detectadas.

  Con las siete categorías de seguridad documentadas, se pretende dar un nuevo enfoque de seguridad a los activos tecnológicos y de información con los que cuenta la SECAB.

- Finalmente se estructura una propuesta que permita tomar decisiones y medidas para salvaguardar los activos tecnológicos y de información dentro de la SECAB, mitigando los riesgos a los que se enfrenta.

BIBLIOGRAFIA

1. ASOCIACIÓN ESPAÑOLA PARA LA CALIDAD (AEC). Seguridad de la información. Centro Conocimiento. Madrid. España. [Consultado 20 Oct, 2014]. Disponible en: http://www.aec.es/web/guest/centro-conocimiento/seguridad-de-la-informacion

2. Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC). Referencias documentales para fuentes de información electrónicas, NTC 4490.1998. P. 5-22. I.C.S.:01.140.20

3. Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC). Código de práctica para la gestión de la seguridad de la información. Bogotá. NTC ISO/IE 27002. 2007. Disponible en: http://oposcaib.wikispaces.com/file/view/39+-+Codi+de+bones+pr%C3%A0ctiques+per+a+la+gesti%C3%B3+de+la+seguretat+de+la+informaci%C3%B3.+Norma+UNE-ISO_IEC+17799.pdf

4. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY [Instituto Nacional De Estándares y Tecnología]. SPECIAL PUBLICACION 800-12: AN INTRODUCTION TO COMPUTER SECURITY: THE NIST HANBOOK [en línea]. [Consultado 25 Oct, 2014]. Disponible en <http://csrc.nist.gov/publications/nistpubs/800-12/800-12-html/chapter1.html>

ANEXOS

ANEXO A. Encuesta realizada dentro de la organización

CLASIFICACION Y CONTROL DE ACTIVOS					
	NO EXISTE	MANUAL	AUTOMATIZADO		
Como es la gestion de activos de informacion? (bases de datos, archivos y documentacion)		X	X		
Como es la gestion de activos de software? (Aplicaciones, Sistemas operativos, herramientas de desarrollo)			X		
Como es la gestion de activos fisicos? (Equipos de computo, comunicaciones, medios magneticos)		X			
Como es la gestion de servicios informaticos? (calefaccion, iluminacion, electricidad)			X		
Existe una gestion de la Clasificacion de los activos de la informacion basado en la sensibilidad y criticidad de la misma?	X				
Basado en dicha clasificacion, existen niveles de proteccion de los activos de la informacion?		X			
Existe un procedimiento de manejo para la informacion de acuerdo a su clasificacion?					
Existe un responsable de clasificar segun su criticidad los activos de la informacion?	SI		NO	X	
SEGURIDAD DEL PERSONAL					
Existe un plan de capacitacion y educacion continua del personal de la empresa con respecto a la seguridad de la informacion?	SI		NO	X	
El personal cuenta con acceso a documentos relacionados con las politicas y procesos de seguridad informatica?	SI	X	NO		
Existe un compromiso de confidencialidad de la informacion firmado por el personal y usuarios externos?	SI	X	NO		
Existe algun mecanismo para promover la comunicacion de debilidades existentes e incidentes ocurridos dentro de la organizacion?	SI		NO	X	
SEGURIDAD FISICA Y AMBIENTAL					
Existe una gestion de accesos a las instalaciones de la compañia?	SI	X	NO		cuales son?
Se cuenta con algun tipo de seguridad para el acceso a los equipamiento de procesamiento de informacion critica?	SI	X	NO		cuales son?
Existe algun tipo de proteccion de factores ambientales que puedan afectar el equipo de computo? (incendios)	SI	x	NO		cuales son?
Existe alguna herramienta de respaldo de la informacion?	SI	x	NO		cuales son?
Existen protocolos de autenticacion para que los usuarios accedan a la informacion?	SI	x	NO		
Existe alguna normativa referente a la seguridad de la informacion	SI	x	NO		

ANEXO A (Continuación)

GESTION DE COMUNICACIONES Y OPERACIONES (SEGURIDAD LOGICA)					
Existe un control en la red de datos contra el software malicioso (virus, troyanos, etc)	SI	x	NO		
Cuentan con procedimientos para prevención de estas amenazas?	SI	x	NO		
Existe una gestión de seguridad en las comunicaciones de la compañía?	SI	x	NO		
Cuentan con un registro de fallas de las comunicaciones de datos?	SI		NO	x	
Cuentan con controles de seguridad para la información en tránsito, utilizado por los canales de comunicación de la compañía?	SI	x	NO		
Cuentan con procedimientos y responsabilidades operativas del uso a los sistemas informáticos?	SI		NO	x	
DESARROLLO Y MANTENIMIENTO DE SISTEMAS					
	NO EXISTE	**MANUAL**	**AUTOMATIZADO**		
Existen gestion de accesos sobre la informacion de la compañía?		X			
Existen normas y procedimientos aplicables durante el ciclo de vida de infraestructura y aplicaciones?	X				
GESTION DE INCIDENCIAS					
	NO EXISTE	**MANUAL**	**AUTOMATIZADO**		
Existe algun reporte de eventos y debilidades de seguridad de la informacion?	X				
Existe gestion de incidentes y mejoras en la seguridad de la informacion?	X				
GESTION DE LA CONTINUIDAD DEL NEGOCIO					
Ante una eventualidad que pueda paralizar total o parcialmente la actividad informática dentro de la empresa, ¿Se tienen medidas y/o procedimientos de neutralización y recuperación?		X			
CONTROL DE ACCESOS					
Cuentan con políticas y procedimientos de control de acceso a los sistemas informáticos de los usuarios internos ?	SI	x	NO		
Cuentan con una administración de acceso a los sistemas informáticos de la compañía?	SI		NO	x	
Cuentan con mecanismos de autenticación y autorización en la compañía?	SI	x	NO		
Existe un registro y monitoreo permanente de acceso a los sistemas informáticos?	SI		NO	x	
Existe políticas de uso para los sistemas de información?	SI		NO	x	
Cuentan con controles de seguridad para los computadores de la compañía?	SI	x	NO		

ANEXO A (Continuación)

Basado en su conocimiento de la estructura distribución y organización relacionados con el sistema de información en la empresa:					
Se cuenta con la información de qué activos se encuentran en mayor peligro?	**SI**	X	**NO**		
Existe una claridad de los posibles eventos que puedan afectar el sisitema de información de la organización, y la probabilidad de ocurrencia?	**SI**	X	**NO**		
Se cuenta con personal encargado responsable de la contingencia en caso de presentar alguna eventualidad?	**SI**	X	**NO**		
En caso de presentarse una eventualidad o desastre natural, se tienen determinados los tiempos de respuesta en los cuales deberán quedar los servicios de información restablecidos ó normalizados?	**SI**		**NO**	X	
PLAN DE SEGUIMIENTO Y MONITOREO					
Teniendo en cuenta los aspectos de seguridad implementados actualmente, se dispone de un proceso de seguimiento del cumplimiento de las politicas de seguridad establecidas?	**SI**		**NO**	X	
En caso de presentarse un incidente de seguridad, se realiza retroalimetación y/o seguimiento con los agentes implicados en el mismo?	**SI**	X	**NO**		
Se cuenta en la organización con alguna herramienta de monitoreo que brinde alarmas e información en caso de presentar un evento de seguridad?	**SI**	X	**NO**		

Fuente: La autora

ANEXO B. Inventario de Activos SECAB

Equipos de Escritorio

GENERAL							CPU			
NOMBRE	CONTRATO	USUARIO RED	EQUIPO	IP	S.O	OFIMATICA	MARCA	MODELO	SERIAL	PLACA
Mónica López	Planta	mlopez	Escritorio	192.168.0.32	WINDOWS 8	2013	HP	PAVILION AIO PC	3CR2450ZJ9	T014
Dayanna Torres	Planta	dtorres	Escritorio	192.168.0.34	Windows XP	2007	HP	COMPAQ DC5850	MXJ83200RQ	T015
Mónica Lozano	Planta	mlozano	Escritorio	192.168.0.36	WINDOWS 8	2013	HP	PAVILION AIO PC	3CR2450ZW2	T025
Zabrina Welter	Contratista	zwelter	Escritorio	192.168.0.40	Windows XP	2007	DELL	PRECISION 390	FWCX281	T022
Jhon Felipe Rocha	Contratista	jrocha	Escritorio	192.168.0.23	Windows XP	2007	DELL	PRECISION 380	8G3LX91	T020
Stella Quinayas	planta	squinayas	Escritorio	192.168.0.35	Windows XP	2007	DELL	PRECISION 390	2XCXZB1	T024
Silvia Moreno	Contratista	smoreno	Escritorio	192.168.0.44	Windows XP	2007	DELL	PRECISION 390	CWCXZB1	T021
Diana Rey	planta	drey	Escritorio	192.168.0.42	WINDOWS 8	2013	HP	PAVILION AIO PC	3CR2450ZTX	T016
Laura Rivera	Contratista	lrivera	Escritorio	192.168.0.43	Windows XP	2007	DELL	PRECISION 380	6G3LX91	T023
Diana Cifuentes	Contratista	dcifuentes	Escritorio	192.168.0.75	Windows XP	2007	DELL	PRECISION 390	HWCXZB1	T019
Olga Turbay	Planta	oturtbay	Escritorio	192.168.0.27	Windows XP	2007	DELL	PRECISION 390	DWCXZB1	T017
Sonia Urueña	Contratista	smuruena	Escritorio	192.168.0.31	WINDOWS 8	2013	HP	PAVILION AIO PC	3CR2450ZHN	T009
Angelica Arciniegas	Planta	aarciniegas	Escritorio	192.168.0.21	Windows XP	2007	DELL	PRECISION 390	4BL99C1	T010
Angelica Arciniegas	Planta	aarciniegas	Escritorio	192.168.0.20	Windows XP	2007	HP	VECTRA XE320	MX21130158	T011
Ciro Sarmiento	Planta	csarmiento	Escritorio	192.168.0.22	Windows XP	2007	DELL	PRECISION 380	9G3LX91	T012
Zenaida Sanmiguel	Planta	zsanmiguel	Escritorio	192.168.0.29	Windows XP	2007	DELL	PRECISION 390	GWCXZB1	T006
Mario Mendoza	Contratista	mmendoza	Escritorio	192.168.0.41	WINDOWS 8	2013	HP	PAVILION AIO PC	3CR2450ZHJ	T018
Juanita Renjifo	Contratista	jrenjifo	Escritorio	192.168.0.26	Windows XP	2007	DELL	PRECISION 390	5BL99C1	T008
Catalina Bateman	Contratista	cbateman	Escritorio	192.168.0.37	Windows XP	2007	HP	COMPAQ DX2300	MXL72307NM	T003
María Alejandra Suarez	Contratista	msuarez	Escritorio	192.168.0.30	Windows XP	2007	HP	WX4400 WORKSTATION	2UA7090FZP	T004
Monica Camargo	Planta	mcamargo	Escritorio	192.168.0.39	WINDOWS 8	2013	HP	PAVILION AIO PC	3CRR24502JN	T005
Nataliza Chaves	Contratista	nchaves	Escritorio	192.168.0.55	Windows XP	2007	LENOVO	MTM-9684	LX0CEHB	T007
Heriberto Caviedes	Planta	hcaviedes	Escritorio	192.168.0.24	Windows XP	2007	HP	DX2000	MXD51606YZ	T001
Heriberto Caviedes	Planta	hcaviedes	Escritorio	192.168.0.76	Windows XP	2007	HP	D220 MT	MXD32701N4	T002

ANEXO B (Continuación)

Monitor, teclado y mouse

	MONITOR				TECLADO			MOUSE		
NOMBRE	MARCA	MODELO	SERIAL	PLACA	MARCA	SERIAL	TIPO	MARCA	SERIAL	TIPO
Mónica López	INTEGRADA				HP	BCXRC0AVB3L1SC	INALÁMBRICO	HP	FCSDF0A263L1SC	INALÁMBRICO
Dayanna Torres	DELL	1907FP	696-AE51	M015	DELL	671-1X3Q	USB	COMPAQ	NO TIENE	PS2
Mónica Lozano	INTEGRADA				HP	BCXRC0AVB3L1YT	INALÁMBRICO	HP	FCSDF0A263L1YT	INALÁMBRICO
Zabrina Welter	DELL	1707	71K-GB4L	M022	DELL	696-1BB9	USB	DELL	HC6320A2Q3R	USB
Jhon Felipe Rocha	LENOVO		VLXC687	M020	HP	C0305042114	PS2	HP	FB7330AN3UI1RSQ	PS2
Stella Quinayas	DELL	1907FP	62M-BAA7	M024	DELL	696-1BB7	USB	LOGITECH	LNA13601495	USB
Silvia Moreno	DELL	1707FP	68G-08PU	M021	DELL	68N-0DK8	USB	HP	NO TIENE	PS2
Diana Rey	INTEGRADA				HP	BCXRC0AVB3L1UG	INALÁMBRICO	HP	FCSDF0A263L1UG	INALÁMBRICO
Laura Rivera	HP	L1706	CND6452RRR	M023	DELL	696-1BB5	USB	LENOVO	4438135	USB
Diana Cifuentes	DELL	1707FP	63H-BG02	M019	DELL	68N-0ILM		DELL	NO TIENE	
Olga Turbay	DELL	1707FP	68E-50SA	M017	LENOVO	1242757	USB	HP	LZE12800479	USB
Sonia Urueña	INTEGRADA				HP	BWWN0DVB2C6BL	INALÁMBRICO	HP	FBXTA0D232C6BX	INALÁMBRICO
Angelica Arciniegas	DELL	1907FP	5C7-B900	M010	DELL	696-1BB4	USB	HP	NO TIENE	USB
Angelica Arciniegas	DELL	1907FP	62M-AHL8	M011	HP	C0305041969	PS2	HP	FB7330AN3UI1RT2	PS2
Ciro Sarmiento	DELL	1907FP	62M-BA9B	M012	HP	BC3370BVBUH4WZ	PS2	DELL	NO TIENE	USB
Zenaida Sanmiguel	DELL	1907FP	62M-AGEZ	M006	DELL	616-07KV	USB	HP	FB7330AN3UI1SF8	PS2
Mario Mendoza	INTEGRADA				HP	BCXRC0AVB3L192	INALÁMBRICO	HP	FCSDF0A263L192	INALÁMBRICO
Juanita Renjifo	DELL	1707FP	63K-0MPS	M008	HP	C0306064373	PS2	DELL	NO TIENE	USB
Catalina Bateman	SAMSUNG	2243LNX	MY22H9NQ803605	M003	DELL	68V-0P4R	USB	MICROSOFT	NO TIENE	USB
María Alejandra Suarez	DELL	1907FP	6AI-AA39	M004	DELL	E145614	USB	DELL	HC6320A2Q2G	USB
Monica Camargo	INTEGRADA				HP	BCXRC0AVB3L1SB	INALÁMBRICO	HP	FCSDF0A263L1SB	INALÁMBRICO
Nataliza Chaves	HP	L1706	CNC721RG78	M007	DELL	69C-0ESS	USB	HP	FB7330AN3UI1SCT	PS2
Heriberto Caviedes	DELL	1707FP	71KGBS6	M001	HP	BC3370BVBUH783	PS2	HP	30512528	PS2
Heriberto Caviedes	DELL	1907FP	62MBA3M	M002	DELL	961BB3	PS2	LOGITECH	N/A	USB

Portátiles

NOMBRE	MARCA	MODELO	SERIAL	PLACA	S.O
Stella Quinalla	LENOVO	YOGA 13	EB331310	P002	WINDOWS 8
Monica Lopez	TOSHIBA	PORTEGE Z835	3C119179	P003	WINDOWS 7
Conferencias	DELL	LATITUDE	6BX-0160	P004	WINDOWS XP
SECAB	LENOVO	IDEAPAD U310	QB073498	P001	WINDOWS 8
SECAB	DELL	INSPIRION 600M	4C2-6023	P005	WINDOWS XP

ANEXO B (Continuación)

Impresoras

MARCA	MODELO	IP	SERIAL	PLACA
HP	LASERJET 1200 SERIES	LOCAL - ZSANMIGUEL	USCB622193	I001
HP	LASERJET 4100N	LOCAL - AARCINIEGAS	USBNK01004	I002
HP	LASERJET 4100N	192.168.0.112	USJNK42532	I003
CANON	IMAGECLASS MF4770N	192.168.0.47	NXV10752	I004
HP	LASERJET 1200 SERIES	LOCAL - MLOPEZ	USCB622211	I005
HP	LASERJET 1200 SERIES	LOCAL - DTORRES	CNCL005089	I006

Otros dispositivos

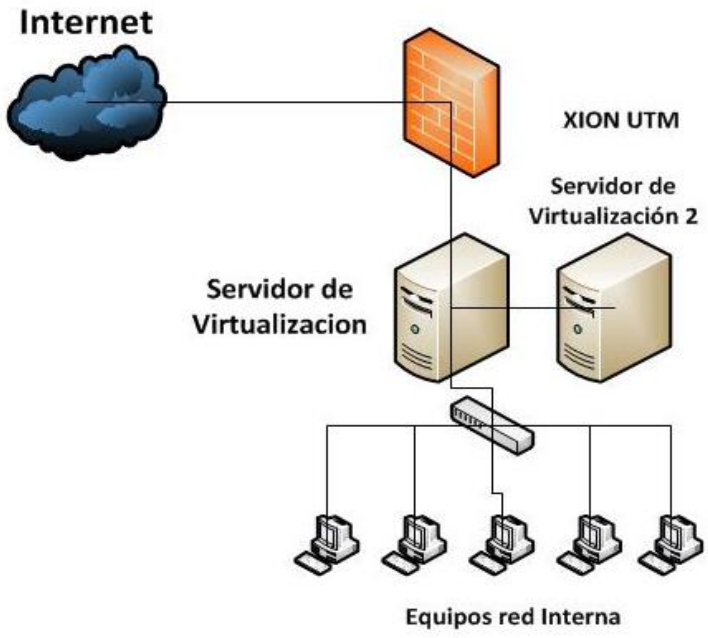
ACCES POINT	Access Point	dlink dwl-2000ap+	D-LINK DWL-2000AP+
MODEM	MODEM	Cuarto Sistemas	PT-LINK
SWITCH	SWITCH	Sistemas	DELL POWER CONNECT 6224
SWITCH	SWITCH	Sistemas	DELL POWER CONNECT 6224
VIDEO BEAM	Proyector	Sala de Integración	BEN-Q

Servidores y sistemas de Información

MARCA	MODELO	IP	PROCESADOR	DISCO DURO	MEMORIA	VIRTUALIZADOS
DELL	POWEREDGE T620	192.168.0.1	INTEL XEON CPU E5-2643 - 3,30 GHZ	1 TB	16 GB	3 ACTIVOS
HP	PROLIANT ML370 G5	192.168.0.2	INTEL XEON CPU E5335 - 2,00 GHZ	1 GB	16 GB	2 ACTIVOS

Actualmente la SECAB cuenta con 2 servidores físicos y un equipo UTM, los cuales se encuentran en el cuarto de servidores desplegándose de la siguiente manera:

ANEXO B (Continuación)



- XION UTM: Firewall Actual.
- Servidor 192.168.0.1: este servidor físico cuenta con 3 virtualizados distribuidos así:

1. Aarciniegas: es una copia de los sistemas que se tienen allí almacenados.
2. Servidor Financiera

Sistema Operativo: Windows 2000 Sp4
Nombre de red: financiera.secab.int
Información redes: ip 192.168.0.8
Mk: 255.255.255.0
GW: 192.168.0.254
DNS1: 192.168.0.240
DNS2: 192.168.0.221
Marca y Modelo: Virtualizado

Funcionan varias bases de datos de programas financieros, no registra ningún problema.

3. Servidor KOPERNICO

Sistema Operativo: Windows 2003 Server
Nombre de red: kopernico.secab.int
Información redes:
Red Local: IP 192.168.0.250
Mk: 255.255.255.0
Gw: 192.168.0.245
DNS1: 192.168.0.221
DNS2: 192.168.0.3
Marca y Modelo: Virtualizado
Funciona como DNS de la red y servidor de dominio delegado.
Funcionan varias bases de datos en de aplicaciones propietarias.

- Servidor 192.168.0.2: este servidor físico cuenta con 2 virtualizados distribuidos así:

1. Servidor GALILEO

Sistema Operativo: Windows 2000
Nombre de red: galileo.secab.int
Información redes: Local
IP: 192.168.0.221
Mk: 255.255.255.0
Gw: 192.168.0.245
DNS1: 192.168.0.245
DNS2: 192.168.0.250
Marca y Modelo: Virtualizado
Bases de datos de Docuware y Seven
Bases de datos de programas propietarios

2. Servidor WebServer

Sistema Operativo: Centos 4/5/6 (32-bit)
Nombre de Red:
IP: 192.168.0.254
Gw: 192.168.0.245
DNS1: 192.168.0.245
DNS2: 192.168.0.250
Marca y Modelo: Virtualizado
Funcionan todas las páginas web

Fuente: La autora

ANEXO C. Guía para rotular la información confidencial

Rotulado para cd

ANEXO C (Continuación)

Documentos físicos

ANEXO C (Continuación)

Documentos para enviar por correo electrónico

El documento deberá ir en el papel indicado anteriormente, se debe identificar en el Asunto del correo la palabra confidencial.

Fuente: La autora

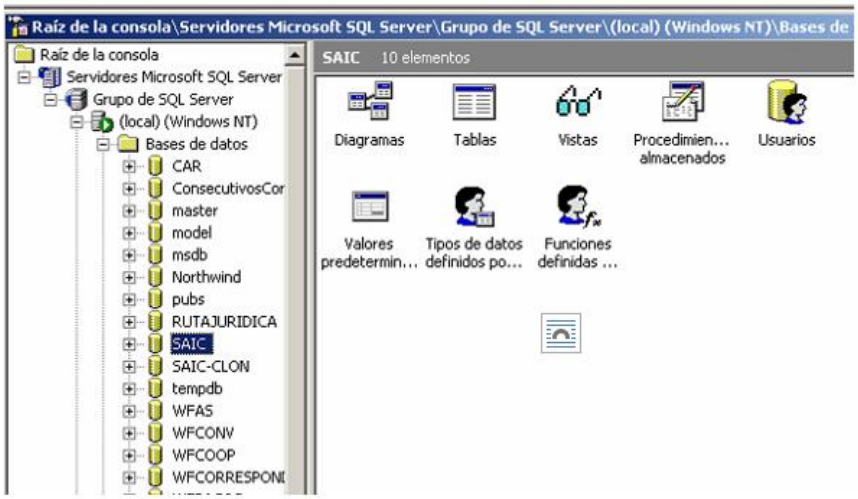
ANEXO D. Procedimientos para Backups

CONVENIO | ANDRES | BELLO
Construimos Ciudadanía para la Integración

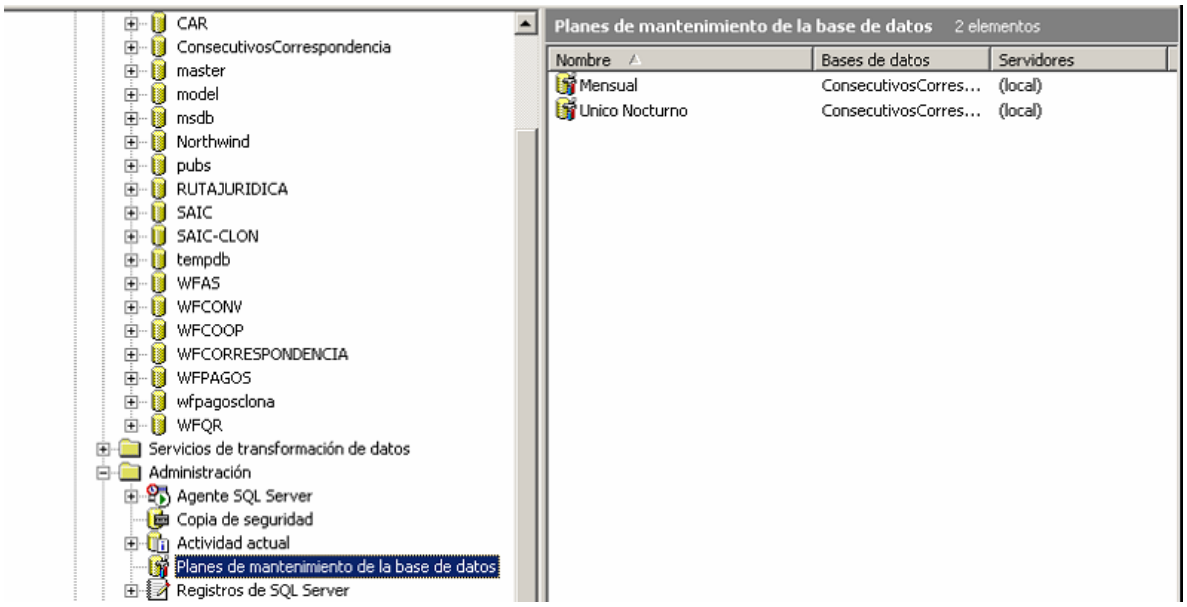
Resumen:
Procedimiento de backup a la base de datos del aplicativo saic

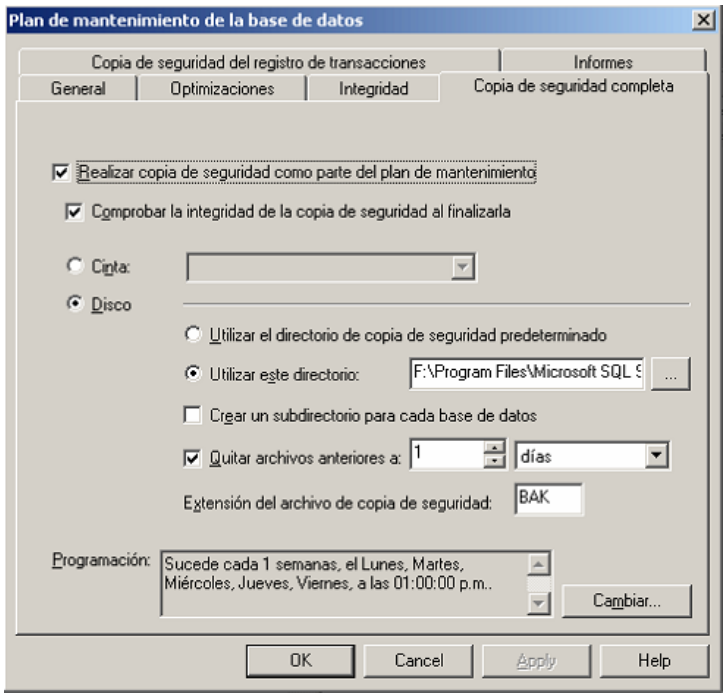
Procedimiento:

Se ingresa al servidor KOPERNICO, se ejecuta el SQL Enterprise Manager se busca la BD SAIC, esta es la base de datos del aplicativo.



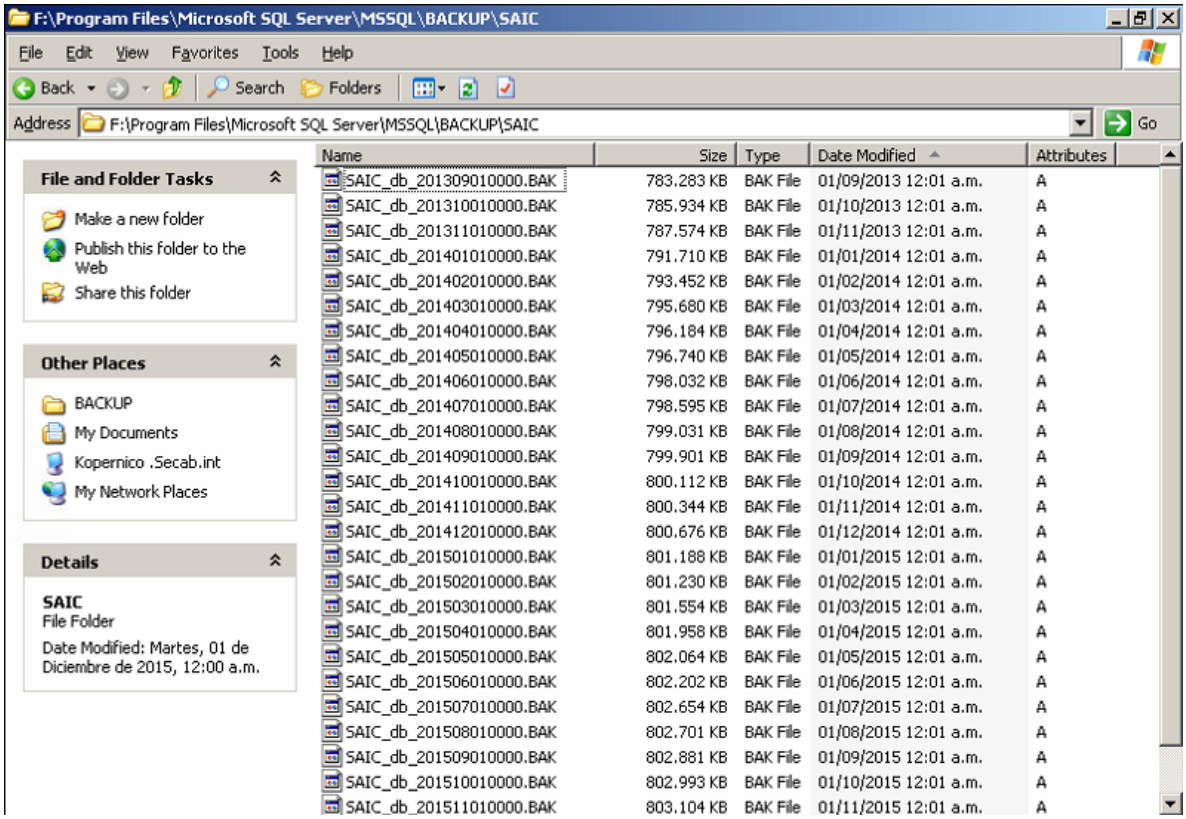
Para ello se encuentra programada una tarea, la cual se ejecuta mensualmente de la siguiente manera:





ANEXO D (Continuación)

La cual queda almacenada según la ruta indicada con la fecha de Backup



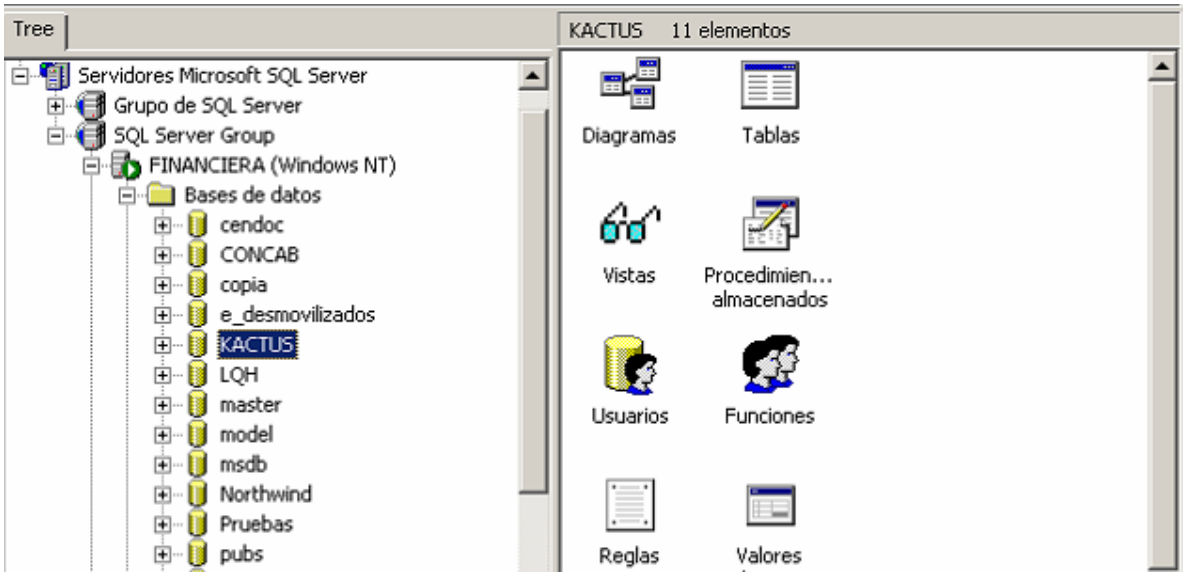
ANEXO D (Continuación)

Resumen:

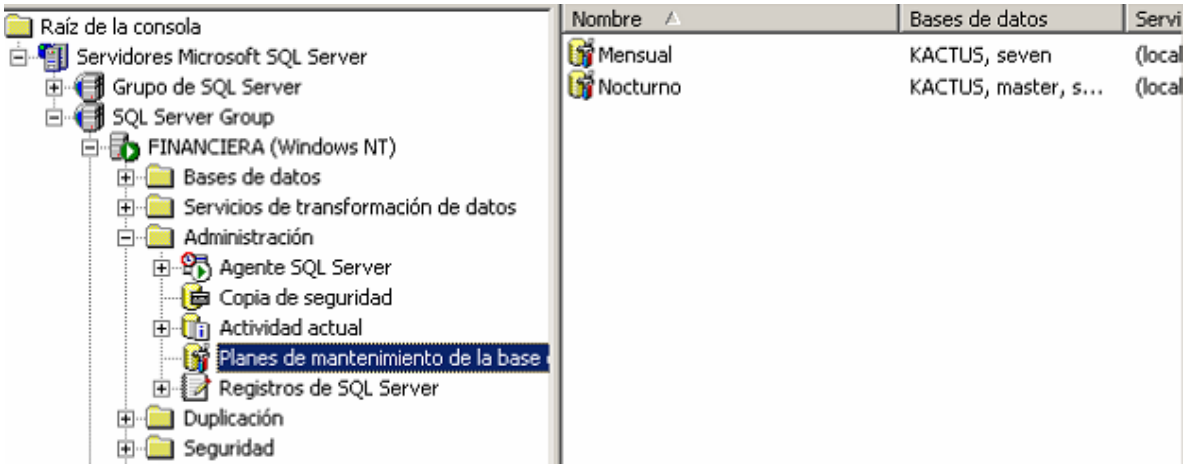
Procedimiento de Backup a la base de datos del aplicativo KACTUS

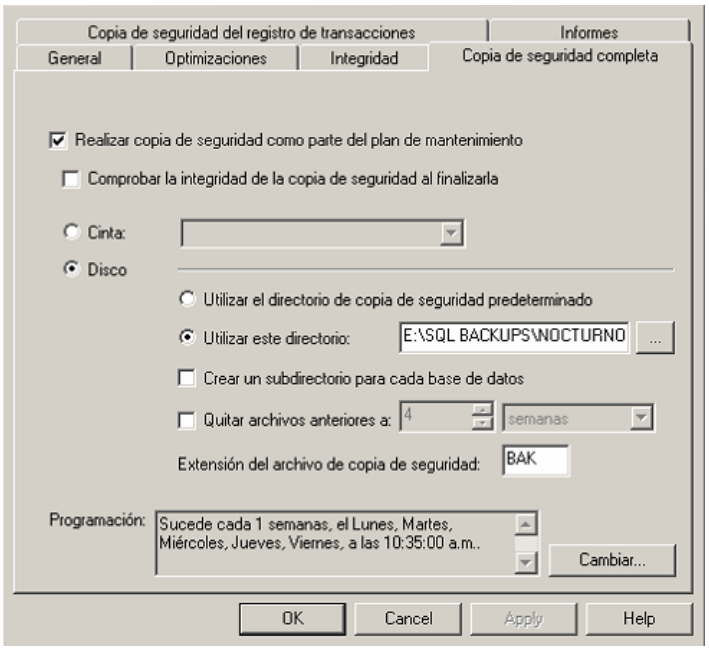
Procedimiento

Se ingresa al servidor FINANCIERA, se ejecuta el SQL Enterprise Manager se busca la BD KACTUS, esta es la base de datos del aplicativo.



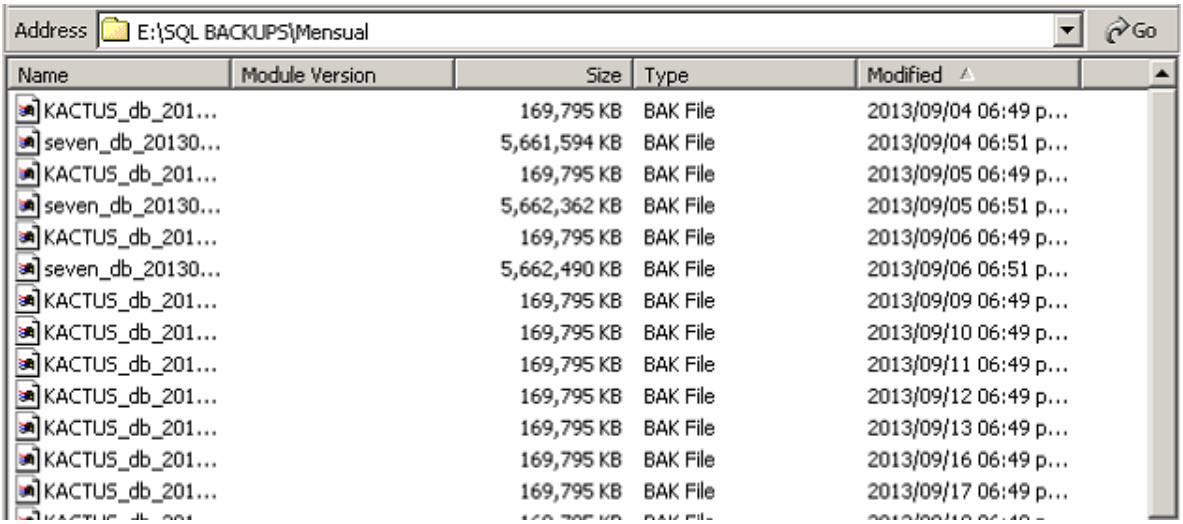
Para ello se encuentra programada una tarea, la cual se ejecuta mensualmente de la siguiente manera:





ANEXO D (Continuación)

La cual queda almacenada según la ruta indicada con la fecha de Backup



Resumen:

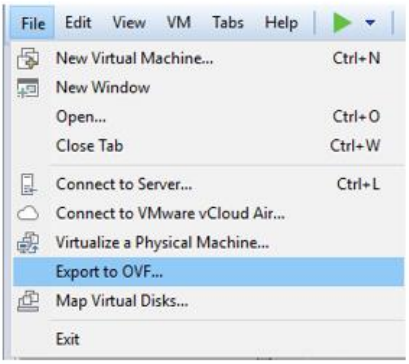
Procedimiento de backup a servidores virtualizados

Procedimiento

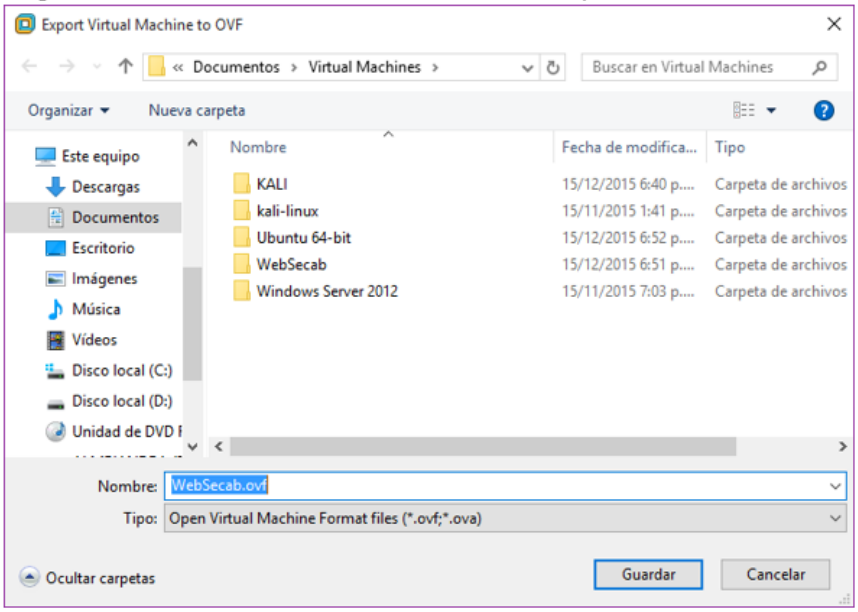
Se ingresa a la consola de WMware en donde se encuentran los servidores virtualizados

- Una vez estén apagados los servidores virtualizados, se ubica el cursor sobre el servidor de la siguiente manera:
  File - Export to OVF

ANEXO D (Continuación)

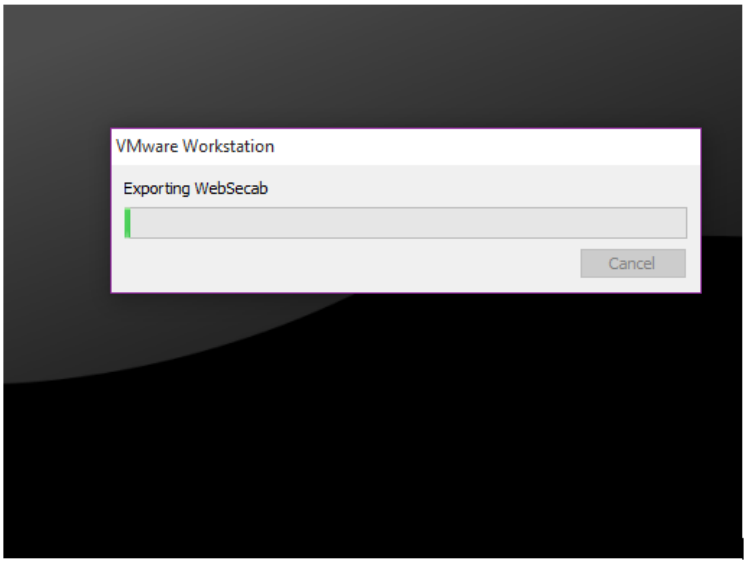


Elegimos la ruta en donde se desea almacenar el Backup



ANEXO D (Continuación)

Toda vez se de click en guardar, se podrá visualizar una ventana con el progreso



Esperamos que este termine para completar el procedimiento.

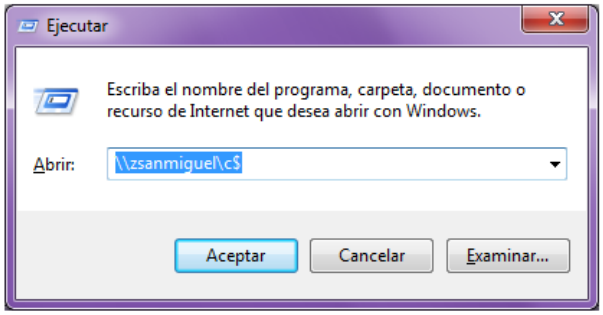
Se realizan el último fin de semana de todos los meses o según sea la consideración

ANEXO D (Continuación)

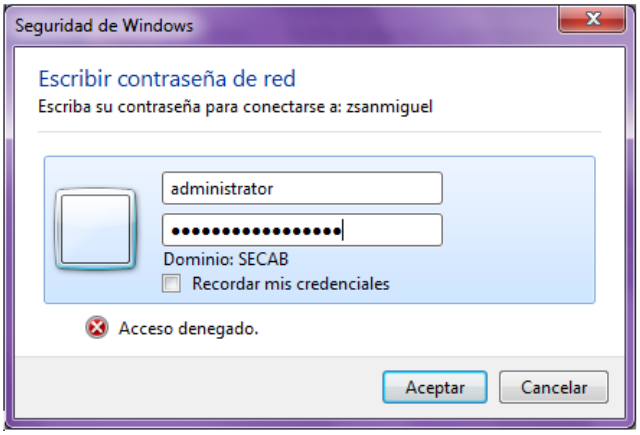
Resumen:
Procedimiento de backup a Usuarios bajo el dominio de la SECAB

Procedimiento:

Se ingresa a la ruta con dirección IP o en su defecto nombre del equipo, todo este procedimiento se realiza bajo la red



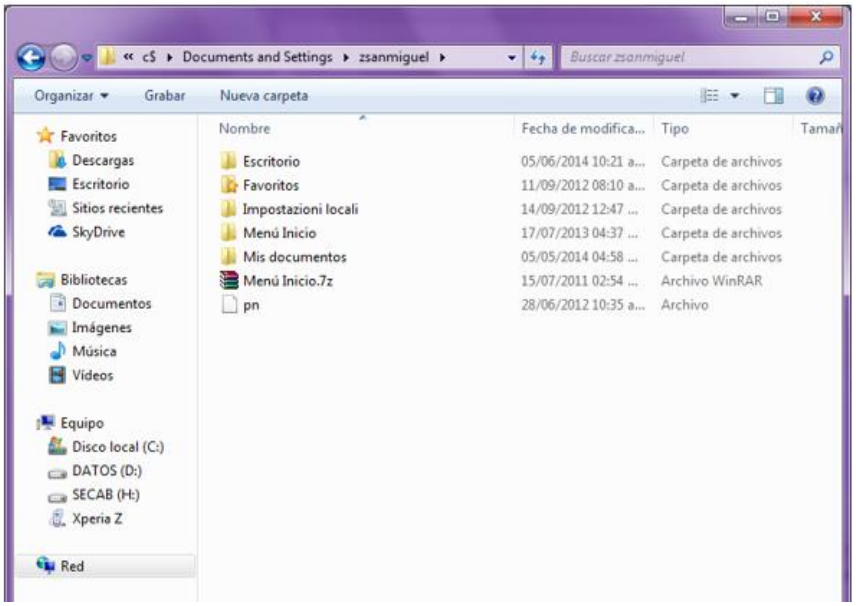
Se ingresa la cuenta Master para el acceso y copia de la información



Luego del acceso a la raíz, se procede a realizar la copia de los archivos que se encuentran que sean institucionales.

No se realiza copia de ningún archivo de música.

Este procedimiento se realiza mensualmente salvaguardando información de los equipos

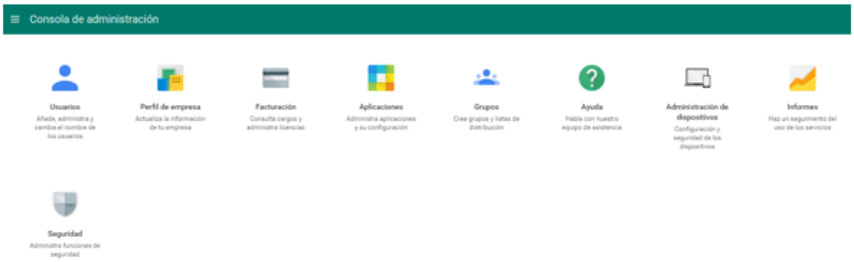


ANEXO E. Creación de Usuarios en Gmail

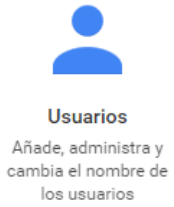
CONVENIO | ANDRES | BELLO
Construimos Ciudadanía para la Integración

Procedimiento

Se ingresa con el usuario administrador de dominio



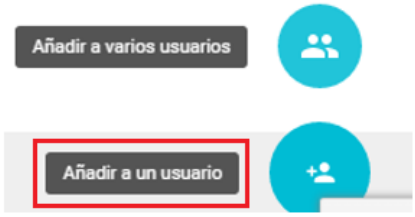
Damos Click en usuarios



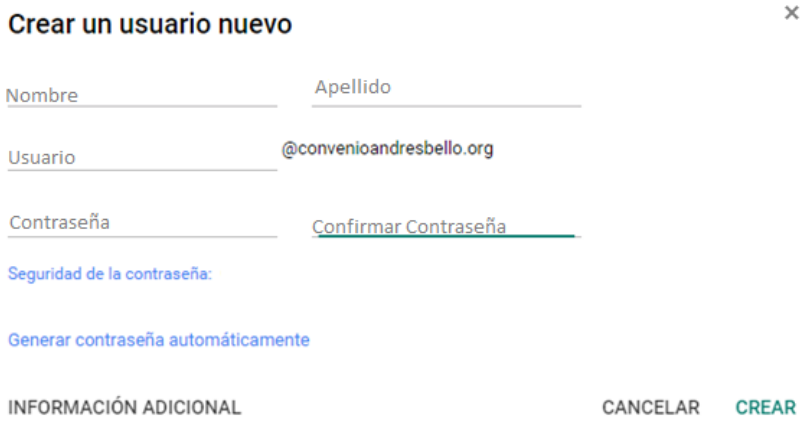
ANEXO E (Continuación)

CONVENIO | ANDRES | BELLO
Construimos Ciudadanía para la Integración

Luego en la parte inferior de la página, damos click en añadir usuarios



En donde aparecerá la siguiente ventana.



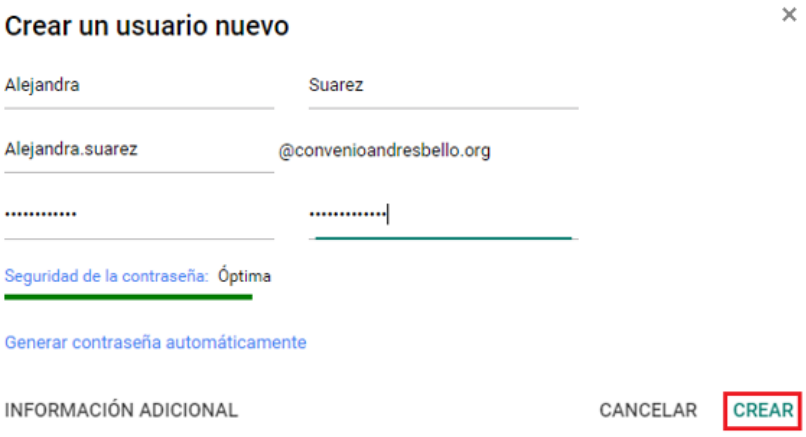
ANEXO E (Continuación)

Diligenciamos los campos con nombre y apellido

En el campo de dirección debemos dejar la primera letra del nombre y el apellido, como se muestra a continuación.

Se establece la contraseña óptima

Por último damos click en crear



Propuesta Plan de Seguridad Informática para la Secretaria Ejecutiva del Convenio Andrés Bello – SECAB

Maria Alejandra Del Pilar Suarez Rojas
Mariaale.suarez@hotmail.com
Especialización Seguridad Informática
Universidad Piloto de Colombia

Resumen – En este artículo se plantea la propuesta de un plan de seguridad informática para mitigar los riesgos y salvaguardar los activos tecnológicos y de información en un organismo internacional, siendo detectadas vulnerabilidades que llegan a ser un riesgo, si son aprovechadas por las diversas amenazas que se encuentran en el entorno.

Luego de realizar un estudio y diagnóstico inicial mediante diversos métodos, se procede a desarrollar un plan basado en parámetros que permitan mitigar los riesgos que se puedan presentar.

Palabras Clave – Amenaza, análisis, mitigar, plan de seguridad, riesgo, vulnerabilidades.

Abstract – This article presents a proposal of a plan of IT security that mitigates the risk as well as protects the technological and information assets in an international organization. This proposal identifies all vulnerabilities that can be a possible threat, it seized by the diverse threats located in the environment. After doing a study and an initial diagnose with different methods this proposal develops a plan based on parameters that allows mitigating all the possible risks.

Key words: Threat, analysis, mitigation, IT security plan, risk, vulnerabilities.

I. INTRODUCCIÓN

Debido a que la información es considerada como el activo de mayor importancia, sin dejar de lado el medio que le contiene, antiguamente dicha información se constituía en papel a lo cual se implementaba una protección física para asegurar dicho activo, pero hoy en día existen diferentes medios para almacenar información, debido a ello nos encontramos con diferentes medios de almacenamiento (medios extraíbles, bases de datos, servidores en la nube, entre otros).

La importancia de este órgano del gobierno se refleja en la información que produce y gestiona, haciéndola un insumo vital que es imprescindible proteger; es por esta razón que se requiere garantizar las condiciones de su eficiencia y eficacia estructurando un modelo de seguridad informática que permita plantear soluciones a diferentes problemáticas que podrían afectar la operación normal de este importante organismo.

En consecuencia que la SECAB no cuenta con ningún tipo de control, ni documentación para casos eventuales a los que se encuentra expuesto por los diferentes riesgos existentes, se busca la aprobación de un plan de seguridad informática dentro de la organización que estructure normativas para minimizar los diferentes riesgos en la infraestructura y la información que puedan ser causadas por las amenazas constantes, aprovechando las vulnerabilidades dentro de la organización, esto sujeto a la aprobación de la Secretaria Ejecutiva y el Ministro presidente.

II. EL CAB.

Es un organismo con personería jurídica internacional, intergubernamental, creada en virtud del Tratado suscrito en Bogotá, el 31 de enero de 1970, sustituido en Madrid en 1990.

Está conformado por 12 Países miembros: Bolivia, Chile, Colombia, Cuba, Ecuador, España, México, Panamá, Paraguay, Perú, República Dominicana y Venezuela. Argentina en proceso de adhesión.

La sede administrativa (SECAB) se encuentra en Bogotá, Colombia y cuenta con tres sedes oficiales en Bolivia el Instituto Internación de Integración (III), en Perú el Instituto de Transferencia de Tecnologías Apropiadas para Sectores Marginales (ITACAB) y en Ecuador el Instituto Iberoamericano de Patrimonio Natural y Cultural (IPANC).

III. OBJETIVO

Proponer un plan de Seguridad Informática que permita desarrollar operaciones seguras; así como, el aseguramiento de la integridad física, el control de los sistemas de información, y la protección de activos de la Secretaría Ejecutiva del Convenio Andrés Bello (SECAB).

IV. CONTENIDO

Con el pasar del tiempo la seguridad informática ha tomado una mayor importancia debido a los avances tecnológicos, las posibilidades de compartir información por medio de la nube, las redes sociales, interconexión entre redes, conexión de dispositivos, han permitido explorar vulnerabilidades en los sistemas lo cual ha conllevado a grandes amenazas para las infraestructuras tecnológicas y su información.

Para ello se deicidio tomar como referencia la ISO 27000 serie, desarrollando la propuesta de la siguiente manera:

A. Diagnóstico

Tras indagación inicial a los ingenieros del área, por medio de encuestas y método de observación, se logran detectar falencias de procesos y políticas que permitan llevar un adecuado manejo de los riesgos frente a los activos tecnológicos y de información.

B. Análisis y Gestión del Riesgo

En esta etapa se realiza un análisis previo, identificando, evaluando y dando un tratamiento a los riesgos que se han sido hallados dentro de la organización. Dando inicio con los criterios y escalas que se van a tener en cuenta para la valoración de los activos, permitiendo enfocar la prioridad que se debe tomar frente a las amenazas y vulnerabilidades, visualizando el impacto y como este se puede mitigar mediante controles.

C. Categorías de Seguridad Desarrolladas

Para la continuidad en el desarrollo del plan de Seguridad Informática, se establecen y documentan 7 categorías estandarizadas tomadas de la norma ISO 27002, las cuales son:

- Política de seguridad: en donde se plantean lineamientos que se deben tener en cuenta a la hora de realizar la aplicabilidad de las políticas de manera formal, frente a los objetivos que sean planteados.
- Organización de la seguridad: las sugerencias allí descritas pretenden estructurar el compromiso, coordinación, responsabilidades y procesos dentro de la organización con respecto a la seguridad y las medidas de prevención frente a las partes externas vinculadas al organismo.
- Gestión de activos: Se propone clasificar la información y establecer responsabilidad de los activos que sean asignados, permitiendo así una protección adecuada de los mismos.

- Seguridad de los recursos humanos: Es importante que las personas vinculadas al organismo sin importar el tipo de relación contractual, tengan claro las responsabilidades frente al tema de la seguridad antes y durante su ingreso y el proceso adecuado a seguir para la selección y retiro del personal.
- Seguridad física y del entorno: Permite establecer uno de los mayores controles en lograr una prevención de pérdidas, robos o alteraciones en los activos tecnológicos encontrados dentro de la SECAB.
- Gestión de operaciones y comunicaciones: Se definen algunos lineamientos procedimentales que permitan una gestión adecuada frente a los procedimientos de gestión, planificación, protección, manejo de medios y las herramientas o diversos medios que se utilicen para el intercambio de la información.
- Control de acceso: Se realizan una serie de sugerencias para que al momento de definir las políticas se tengan en cuenta el modo de acceso para los usuarios, como se debe realizar los registros, la asignación de privilegios y contraseñas que estos deban tener, no obstante que los mismos preserven el buen uso y la responsabilidad.

En cada una de las categorías tomadas, se realizan propuestas desde el punto de vista de la seguridad, que permitan dar lineamientos de la estructuración que deben tomar en la elaboración del plan de seguridad informática dentro de la organización

V. CONCLUSIÓN

La información por ser el activo más importante, requiere de planes eficientes que permitan minimizar los riesgos ante las diversas vulnerabilidades, luego del análisis realizado, se determina que la SECAB no cuenta con los controles necesarios dentro del organismo y pese a las diversas administraciones en el área de sistemas, nunca se han presentado planes de mejora o en algún otro caso los riesgos a los que se encuentran expuestos por las vulnerabilidades detectadas.

Con las siete categorías de seguridad documentadas, se pretende dar un nuevo enfoque de seguridad a los activos tecnológicos y de información con los que cuenta la SECAB.

REFERENCIAS

[1] INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Norma técnica colombiana para tecnología de la información, técnicas de seguridad. Código de práctica para la gestión de la seguridad de la información. Bogotá D.C.. ICONTEC. 2007 NTC-ISO/IEC 72002